



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise, with the Verizon Business Private IP (PIP) IP Trunk service.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

The Verizon Business IP Trunk service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	7
2.3.	The SIP Trunk Redundant (2-CPE) Architecture Option	7
2.4.	Support.....	8
2.4.1	Avaya	8
2.4.2	Verizon.....	8
2.5.	Known Limitations	8
3.	Reference Configuration	9
3.1.	History-Info and Diversion Headers	11
4.	Equipment and Software Validated	11
5.	Configure Avaya Communication Server 1000E	12
5.1.	Node and Key IP Addresses	13
5.2.	Virtual D-Channel, Routes and Trunks	16
5.2.1	Virtual D-Channel Configuration	16
5.2.2	Routes and Trunks Configuration.....	17
5.3.	SIP Trunk to Session Manager	20
5.4.	Routing of Dialed Numbers to Session Manager	26
5.4.1	Route List Block	26
5.4.2	NARS Access Code	28
5.4.3	Numbering Plan Area Codes	29
5.4.4	Other Special Numbers to Route to Session Manager.....	30
5.5.	Zones	31
5.6.	Codec Parameters, Including Ensuring Annexb=no for G.729	34
5.6.1	Media Gateway Configuration.....	34
5.6.2	Node Voice Gateway and Codec Configuration.....	35
5.7.	Enabling Plug-Ins for Call Transfer Scenarios	37
5.8.	Customer Information	38
5.8.1	Caller ID Related Configuration.....	39
5.9.	Example CS1000E Telephone Users	41
5.9.1	Example IP UNISim Phone DN 2000, Codec Considerations	41
5.9.2	Example SIP Phone DN 2900, Codec Considerations.....	42
5.9.3	Example Digital Phone DN 2222	43
5.9.4	Example Analog Port with DN 2221, Fax	44
5.10.	Save Configuration	45
6.	Configure Avaya Aura® Session Manager	46
6.1.	SIP Domain	48
6.2.	Locations.....	49
6.2.1	Location for Avaya Communication Server 1000E.....	49
6.2.2	Location for Avaya SBC For Enterprise.....	50
6.3.	Configure Adaptations	52
6.3.1	Adaptation for Avaya Communication Server 1000E.....	52
6.3.2	Adaptation for Avaya SBC for Enterprise	54

6.4.	SIP Entities.....	55
6.4.1	SIP Entity for Avaya Communication Server 1000E	55
6.4.2	SIP Entity for Avaya SBC for Enterprise	56
6.5.	Entity Links.....	57
6.5.1	Entity Link to Avaya Communication Server 1000E	57
6.5.2	Entity Link to Avaya SBC for Enterprise	58
6.6.	Routing Policies	59
6.6.1	Routing Policy to Avaya Communication Server 1000E	59
6.6.2	Routing Policy to Avaya SBC for Enterprise	59
6.7.	Dial Patterns.....	60
6.7.1	Inbound Verizon Calls to CS1000E Users.....	60
6.7.2	Outbound Calls to Verizon	61
7.	Configure Avaya Session Border Controller for Enterprise	63
7.1.	Access the Management Interface	63
7.2.	Device Specific Settings	65
7.2.1	Define Network Information.....	65
7.2.2	Signaling Interfaces	66
7.2.3	Media Interfaces.....	67
7.3.	Global Profiles	68
7.3.1	Routing Profiles	68
7.3.2	Topology Hiding Profile	69
7.3.3	Server Interworking	71
7.3.4	Signaling Manipulation.....	74
7.3.5	Server Configuration.....	76
7.3.6	Server Configuration for Verizon IP Trunk.....	78
7.4.	Domain Policies – Application Rule.....	80
7.5.	Domain Policies – Media Rules.....	81
7.6.	Domain Policies – Signaling Rules.....	83
7.7.	Domain Policies – End Point Policy Groups	84
7.8.	Device Specific Settings – End Point Flows.....	86
8.	Verizon Business IP Trunk Service Offer Configuration	89
8.1.	Fully Qualified Domain Name (FQDN)s	89
8.2.	DID Numbers Assigned by Verizon	89
9.	Verification Steps.....	90
9.1.	Avaya Communication Server 1000E Verifications.....	90
9.1.1	IP Network Maintenance and Reports Commands	90
9.1.2	System Maintenance Commands.....	95
9.2.	Wireshark Verifications	96
9.2.1	Example Outbound Call.....	96
9.2.2	Example Inbound Call	99
9.3.	System Manager and Session Manager Verification	102
9.3.1	Verify SIP Entity Link Status	102
9.4.	Avaya Session Border Controller for Enterprise Verification	103
9.4.1	Welcome Screen	103
9.4.2	Alarms.....	103
9.4.3	Incidents	104

9.4.4	Tracing	105
10.	Conclusion	106
11.	Additional References	107
11.1.	Avaya	107
Appendix 1:	Sigma Script.....	108

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E (CS1000E) Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise (ASBCE), with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls via standards-based SIP trunks.

Avaya CS1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

Customers using Avaya CS1000E with the Verizon Business IP Trunk SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

Verizon Business IP Trunk service offer can be delivered to the customer premise via either a Private IP (PIP) or Internet Dedicated Access (IDA) IP network terminations. Although the configuration documented in these Application Notes used Verizon's IP Trunk service terminated via a PIP network connection, the solution validated in this document also applies to IP Trunk services delivered via IDA service terminations.

For more information on the Verizon Business IP Trunking service, including access alternatives, visit <http://www.verizonbusiness.com/us/products/voip/trunking/>

2. General Test Approach and Test Results

The Avaya CS1000E location was connected to the Verizon Business IP Trunk Service, as depicted in **Figure 1**. The Avaya equipment was configured to use the commercially available SIP Trunking solution provided by the Verizon Business IP Trunk SIP Trunk Service. This allowed Avaya CS1000E users to make calls to the PSTN and receive calls from the PSTN via the Verizon Business IP Trunk SIP Trunk Service.

2.1. Interoperability Compliance Testing

The SIP trunk interoperability testing included the following:

- DNS SRV to determine the Verizon IP Trunk SIP signaling information, using UDP for SIP signaling and full SIP headers. The use of DNS SRV is optional, and the configuration was tested with static configuration of the Verizon SIP signaling IP Address and port as well as with the DNS SRV configuration.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Verizon Business to the Avaya CS1000E location. These incoming PSTN calls arrived via the SIP Trunk and were answered by Avaya SIP telephones, Avaya IP UNISTim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID on

display-equipped Avaya CS1000E telephones was verified. Avaya CS1000E sent 180 Ringing (without SDP) for calls ringing to an Avaya CS1000E telephone user.

- Outgoing calls from the Avaya CS1000E location to the PSTN were routed via the SIP Trunk to Verizon Business. These outgoing PSTN calls were originated from Avaya SIP telephones, Avaya IP UNISim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID on display-equipped PSTN telephones was verified. Outbound calls using “fast answer” (200 OK from Verizon without a preceding 18x) were also tested successfully.
- Proper disconnect when the caller abandoned a call before answer for both inbound and outbound calls.
- Proper disconnect when the Avaya CS1000E party or the PSTN party terminated an active call.
- Proper busy tone heard when an Avaya CS1000E user called a busy PSTN user, or a PSTN user called a busy Avaya CS1000E user (i.e., if no redirection was configured for user busy conditions).
- Various outbound PSTN call types were tested including long distance, international, toll-free, operator assisted, directory assistance, and non-emergency x11 calls.
- Requests for privacy (i.e., caller anonymity) for Avaya CS1000E outbound calls to the PSTN were verified. That is, when privacy was requested by Avaya CS1000E, outbound PSTN calls were successfully completed while withholding the caller ID from the displays of display-equipped PSTN telephones.
- Privacy requests for inbound calls from the PSTN to Avaya CS1000E users were verified. That is, when privacy was requested by a PSTN caller, the inbound PSTN call was successfully completed to an Avaya CS1000E user while presenting an “anonymous” display to the Avaya CS1000E user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both Verizon Business and the Avaya Session Border Controller for Enterprise were able to monitor health using SIP OPTIONS. The ASBCE configurable control of SIP OPTIONS timing was exercised successfully.
- Incoming and outgoing voice calls using the G.729A and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission for incoming and outgoing calls.
- Inbound and outbound long holding time call stability.
- Telephony features such as call waiting, hold, transfer using re-INVITE and conference. Note that CS1000E will not send REFER to the Verizon network.
- Inbound calls from Verizon IP Trunk Service that were call forwarded back to PSTN destinations via Verizon IP Trunk Service, presenting true calling party information to the destination PSTN telephone.
- Proper DiffServ markings for SIP signaling and RTP media.
- Inbound and outbound fax calls.
- Inbound and outbound G.729A voice calls for which intentionally induced ambient fax tone “noise” caused Verizon to issue a re-INVITE to G.711.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations were noted:

- **T.38 Fax:** Verizon has implemented T.38 Fax in their network, however Verizon does not re-invite to T.38 so outbound faxes will completed at G.711.
- **Avaya CS1000E does not support sending REFER:** Incoming Verizon IP Trunk calls that are transferred back out to the PSTN via the Verizon IP Trunk service will continue to traverse the enterprise site (i.e., will not be released via a REFER-based transfer).
- **Transfer from PSTN to PSTN:** Assume a call is active between a CS1000E telephone user and a PSTN user “A”. To allow the CS1000E user to transfer the call using the Verizon IP Trunk service to another PSTN user “B”, patch P30224_1.ntl must be enabled. For the information on how to obtain and apply this patch, please visit <http://support.avaya.com>.
- **Blind transfer off-net, calling party on PSTN does not hear ringback tone when the called PSTN is ringing:** This limitation is encountered when performing a workaround to support a blind transfer call without an UPDATE/SDP method. Before completing the transferred call, the CS1000E uses an UPDATE/SDP method to anchor ring back tone on the 2nd leg to the 1st leg. However, Verizon does not support this method, it rejects the UPDATE/SDP with a “500 Internal Server Error” response. A workaround has been made to eliminate the UPDATE method on inbound signaling, that makes the CS1000E automatically disable UPDATE from being sent to Verizon. This is achieved by the SigMa Script on the ASBCE in **Section 7.3.4** and by enabling plug-in 501 for the CS1000E in **Section 5.7**.
 - **Note:** The CS1000E requires support of UPDATE, but Verizon does not support this method. Not supporting UPDATE may result in significant service degradation and feature breakage.

2.3. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two units of Avaya Session Border Controllers for Enterprise. One ASBCE is designated as Primary and the other as Secondary. The ASBCEs reside at the edge of the customer network.

Session Manager is provisioned to attempt outbound calls to the Primary ASBCE first. If that attempt fails, the Secondary ASBCE is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary ASBCE. If there is no response then the call will be sent to the Secondary ASBCE.

2.4. Support

2.4.1 Avaya

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

2.4.2 Verizon

For technical support on Verizon Business IP Trunk service offer, visit the online support site at <http://www.verizonbusiness.com/us/customer/>.

2.5. Known Limitations

The following limitations are noted for the sample configuration described in these Application Notes:

- Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities 911 capabilities were not tested. It is customer's responsibility to ensure proper operation with its equipment/software vendor.
- Verizon Business IP Trunking service does not support G.729B codec.

Note – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

3. Reference Configuration

Figure 1 illustrates an example Avaya CS1000E solution connected to the Verizon Business IP Trunk SIP Trunk service. The Avaya equipment is located on a private IP network. An enterprise edge router provides access to the Verizon Business IP Trunk service network via a Verizon Business T1 circuit. This circuit is provisioned for the Verizon Business Private IP (PIP) service. The optional Verizon “unscreened ANI” feature is not needed by the Avaya CS1000E, and “unscreened ANI” is not provisioned on the production circuit used for testing.

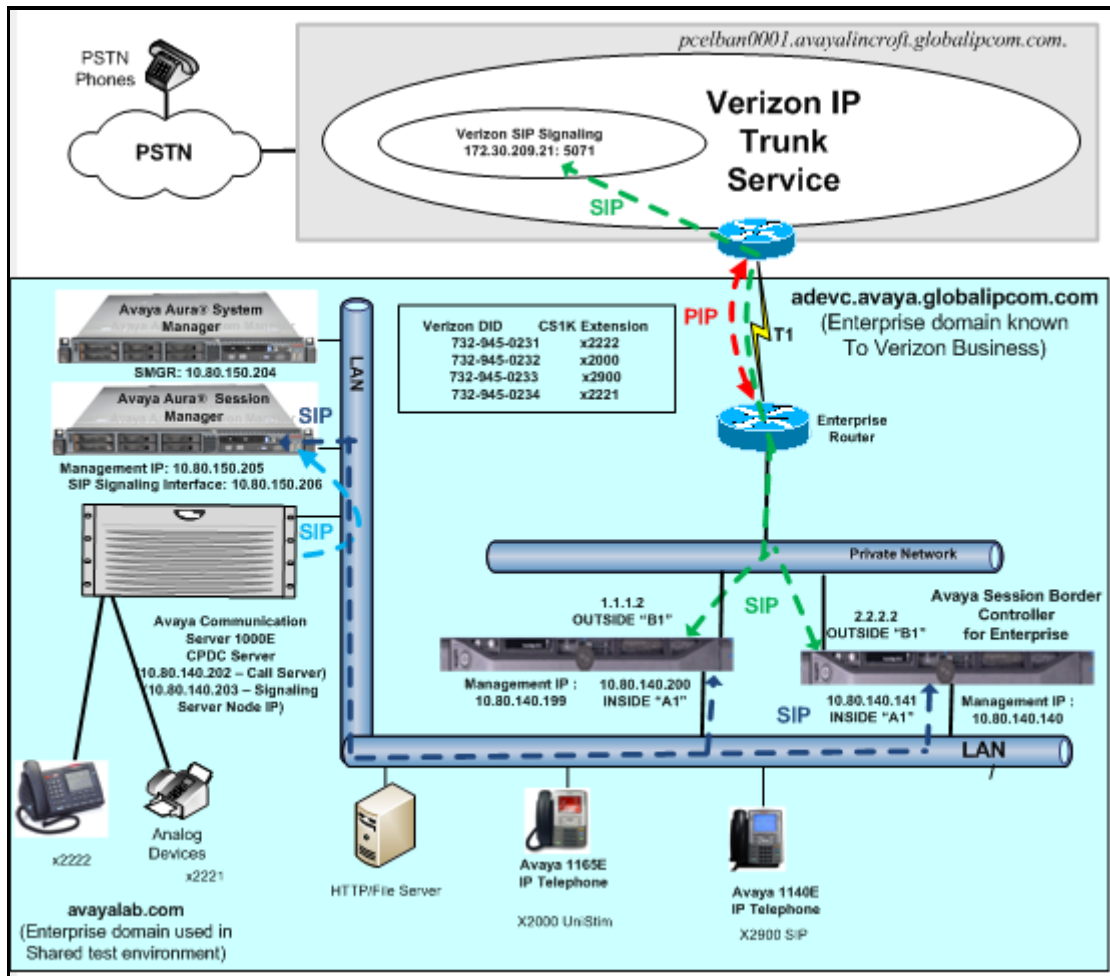


Figure 1: Avaya Interoperability Test Lab Configuration

In the sample configuration, the ASBCE receives traffic from the Verizon Business IP Trunk service on port 5060. When the ASBCE is installed, a static IP Address for the Verizon SIP signaling address and port can be entered. If DNS SRV is preferred, the ASBCE can be configured to use DNS SRV, using UDP for transport, to determine the IP Address and port to be used to send SIP signaling to Verizon. In the sample configuration, the DNS process will result in SIP signaling being sent to IP Address 172.30.209.21 and port 5071.

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk Service as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Session Manager Release 6.1 and Communication Server Release 7.5 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test lab. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avayalab.com” at the enterprise. The ASBCE was used to adapt the “avayalab.com” domain to the domains known to Verizon. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Server and Session Manager match the CPE domain known to the Verizon Business IP Trunk service.

The Verizon Business IP Trunk service provided Direct Inward Dial (DID) numbers that terminated at the Avaya CS1000E location. These DID numbers were mapped to Avaya CS1000E users via a Session Manager adaptation. **Table 1** shows a sample mapping of Verizon-provided DID numbers to CS1000E telephone users.

Verizon Provided DID	Avaya CS1000E Destination	Notes
732-945-0234	x2221	Analog telephone / fax
732-945-0231	x2222	Avaya M3904 Digital Telephone
732-945-0232	x2000	Avaya 1165E IP Deskphone (UNISim)
732-945-0233	x2900	Avaya 1140E IP Deskphone (SIP)

Table 1: Sample Verizon DID to CS1000E Telephone Mappings

The following components were used in the sample configuration:

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the sample configuration shown in **Figure 1**. Verizon Business customers will use different FQDNs and IP addressing as required.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
 - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN)
 - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controller for Enterprise(ASBCE) 4.0.5Q09
- Avaya Communication Server 1000E Release 7.5
- Avaya System Manager Release 6.1
- Avaya Session Manager Release 6.1
- Avaya 1100-Series IP Deskphones using UNISim software
- Avaya 1140E IP Deskphones using SIP software, registered to the CS1000E
- Avaya M3900-Series Digital phones
- Analog telephones and fax machines

3.1. History-Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History-Info Headers. Instead, the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for redirected calls. The Avaya Communication Server 1000E includes History-Info header in messaging sent to Session Manager. Session Manager can convert the History Info header into the Diversion Header required by Verizon. This is performed by specifying the “*VerizonAdapter*” adaptation in Session Manager. See **Section 6.3**.

The Avaya Communication Server 1000E call forwarding feature may be used for call scenarios testing Diversion Header.

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	Release 7.5, Version 7.50.17 (with latest Patches and Deplist) Plug-in 201 Enabled Plug-in 501 Enabled
Avaya Aura® System Manager running on HP Common Server	Release 6.1.0 (Build Number 6.1.0.0.7345 Patch 6.1.5.502)
Avaya Aura® Session Manager running on HP Common Server	Release 6.1 (Load 6.1.5.0.615006)
Avaya Session Border Controller for Enterprise running on Dell R210 V2 server	4.0.5Q09
Avaya 1100-Series IP Deskphones (UNISTim)	FW 0626C8A
Avaya 1140E IP Deskphones (SIP)	SIP 04.03.09.00
Avaya M3900-Series Digital Telephone	N/A
Brother Intellifax 1360	N/A

Table 2: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server and Call Server applications all running on the same CP+DC server platform.

Session Manager Release 6.1 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Service (NRS). As a result, the NRS application is not required to configure a SIP trunk between Avaya Communication Server 1000E and Session Manager Release 6.1.

This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog, digital, UNISim, and SIP telephones

Configuration will be shown using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via **https://<ip-address>** where the relevant <ipaddress> in the sample configuration is 10.80.140.202. The following screen shows an abridged log-in screen. Log in with appropriate credentials.

Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

Go to central login for Single Sign-On

User ID:

Password:

[Change Password](#)

Alternatively, if System Manager has been configured as the Primary Security Server for the Avaya Unified Communications Management application and Avaya Communication Server 1000E is registered as a member of the System Manager Security framework, the Element Manager may be accessed via System Manager. In this case, access the web based GUI of System Manager by using the URL “**http://<ip-address>/SMGR**”, where <ip-address> is the IP address of System Manager. Log in with appropriate credentials. The System Manager Home Page will be displayed. Under the **Services** category on the right side of the page, click the **UCM Services** link (not shown).

The Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the **Element Name** corresponding to “CS1000” in the **Element Type** column. In the abridged screen below, the user would click on the **Element Name** “EM on vz_cs1k”.

Avaya Unified Communications Management

[Help](#) | [Logout](#)

Host Name: 10.80.140.202 Software Version: 02.20.0023.00(5197) User Name admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

<input type="checkbox"/>	Element Name	Element Type ▲	Release	Address	Description ▲
1 <input type="checkbox"/>	EM on vz_cs1k	CS1000	7.5	10.80.141.202	New element.
2 <input type="checkbox"/>	vz_cs1k.avayalab.com (primary)	Linux Base	7.5	10.80.140.202	Base OS element.
3 <input type="checkbox"/>	10.80.141.201	Media Gateway Controller	7.5	10.80.141.201	New element.
4 <input type="checkbox"/>	NRSRM on vz_cs1k	Network Routing Service	7.5	10.80.141.202	New element.

5.1. Node and Key IP Addresses

Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click “<Node id>” in the **Node ID** column to view details of the node. In the sample configuration, **Node ID “1004”** was used.

AVAYA

CS1000 Element Manager

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

Print | Refresh

<input type="checkbox"/>	Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/>	1004	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.203		Synchronized

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- [Nodes: Servers, Media Cards](#)
- Maintenance and Reports
- Media Gateways

The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **Node IPV4 address** under **Telephony LAN (TLAN)**. In the sample screen below, the **Node IPV4 address** is “10.80.140.203”. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E.

CS1000 Element Manager

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1004 - SIP Line, LTPS, Gateway (SIPGw))

Node ID: 1004 * (0-9999)

Call server IP address: 10.80.141.202 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Telephony LAN (TLAN)

Gateway IP address: 10.80.141.1 *
Node IPv4 address: 10.80.140.203 *

Subnet mask: 255.255.255.0 *
Subnet mask: 255.255.255.0 *

Node IPv6 address:

The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader

Print | Refresh

<input type="checkbox"/> Hostname ^	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.80.141.202	10.80.140.202	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

Expand **System** → **IP Network** on the left panel and select **Media Gateways**. Select the media gateway listed, here **'004 00'**. Click **'Next'** (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with 'System' expanded and 'Media Gateways' selected. The main panel displays the 'Media Gateways' configuration page. At the top, it shows 'Managing: 10.80.141.202' and 'Username: admin'. Below this, there's a table with columns: IPMG, IP Address, Zone, and Type. The first row shows '004 00' in the IPMG column, '10.80.141.201' in the IP Address column, '1' in the Zone column, and 'MGS' in the Type column. Above the table, there are buttons for 'Add...', 'Digital Trunking...', 'Reboot', 'Delete', 'Virtual Terminal', and a 'More Actions' dropdown.

The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone to the PSTN via Verizon IP Trunk service, the IP Address in the SDP in the INVITE message will be 10.80.140.204 in the sample configuration.

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'IPMG 4 0 Media Gateway Survivable(MGS) Configuration' page. The left sidebar shows 'System' expanded and 'Media Gateways' selected. The main panel displays the configuration page. Under the 'Media Gateway (MGS)' heading, there are fields for 'Hostname' (MGS), 'Embedded LAN (ELAN) IP address' (10.80.141.201), 'Embedded LAN (ELAN) gateway IP address' (10.80.141.1), 'Embedded LAN (ELAN) subnet mask' (255.255.255.0), 'Telephony LAN (TLAN) IP address' (10.80.140.201), 'Telephony LAN (TLAN) gateway IP address' (10.80.140.1), and 'Telephony LAN (TLAN) subnet mask' (255.255.255.0). Under the 'DSP Daughterboard' heading, there is a dropdown for 'Type of the DSP daughterboard' (DB128) and a field for 'Telephony LAN (TLAN) IP address' (10.80.140.204), which is highlighted with a red rectangle. Below this, the 'Telephony LAN (TLAN) gateway IP address' is set to 10.80.140.1.

5.2. Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

5.2.1 Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **Routes and Trunks**. In the sample configuration, there is a virtual D-Channel 15 associated with the Signaling Server.

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation (N
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks

Managing: **10.80.141.202** Username: admin
Routes and Trunks > Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 64	Add route	
+ Route: 15	Type: TIE	Description: VTKNODE1004SIP	Edit	Add trunk
+ Route: 17	Type: TIE	Description: VTK1004SIPLINE	Edit	Add trunk

5.2.2 Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left navigation panel and expand the customer number. In the example screen that follows, it can be observed that Route 1 has 32 trunks in the sample configuration.

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Software

Customers

Routes and Trunks


Routes and Trunks

D-Channels

Managing: 10.80.141.202 Username: admin2

Routes and Trunks » Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 64	Add route	
 Route: 15	Type: TIE	Description: VTKNODE1004SIP	Edit	Add trunk
+ Trunk: 1 - 32	Total trunks: 32			
+ Route: 17	Type: TIE	Description: VTK1004SIPLINE	Edit	Add trunk

Select **Edit** to verify the configuration, as shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

Customer 0, Route 15 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :

Customer number (CUST) :

Route number (ROUT) :

Designator field for trunk (DES) :

Trunk type (TKTP) :

Incoming and outgoing trunk (ICOG) :

Access code for the trunk route (ACOD) :

Trunk type M911P (M911P) :

The route is for a virtual trunk route (VTRK) :

- Zone for codec selection and bandwidth
management (ZONE) :

- Node ID of signaling server of this route
(NODE) :

- Protocol ID for the route (PCID) :

RDB

00

15

VTKNODE1004SIF

TIE

Incoming and Outgoing (IAO)

7900015

☐

☒

00099

1004

SIP (SIP)

(0 - 8000)

(0 - 9999)

*

Scrolling down, other parameters may be observed. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.2.1**.

Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) :	15 (0 - 254)
- Interface type for route (IFC) :	Meridian M1 (SL1)
- Private network identifier (PNI) :	00001 (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO) :	<input type="checkbox"/>
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :	<input type="checkbox"/>
- Channel type (CHTY) :	B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) :	Unknown Call type (UKWN)
- Insert ESN access code (INAC) :	<input checked="" type="checkbox"/>
- Integrated service access route (ISAR) :	<input type="checkbox"/>
- Display of access prefix on CLID (DAPC) :	<input type="checkbox"/>
- Mobile extension route (MBXR) :	<input type="checkbox"/>
- Mobile extension outgoing type (MBXOT) :	National number (NPA)
- Mobile extension timer (MBXT) :	0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) :	Unknown (UKWN)

5.3. SIP Trunk to Session Manager

Expand **System** → **IP Network** → **Nodes: Servers, Media Cards**. Click “**1004**” in the **Node ID** column (not shown) to edit configuration settings for the configured node.

Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link to view or edit the SIP Gateway configuration.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1004 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *

Node IPv6 address:

IP Telephony Node Properties	Applications (click to edit configuration)
<ul style="list-style-type: none">• Voice Gateway (VGW) and Codecs• Quality of Service (QoS)• LAN• SNTP• Numbering Zones• MCDN Alternative Routing Treatment (MALT) Causes	<ul style="list-style-type: none">• SIP Line• Terminal Proxy Server (TPS)• Gateway (SIPGw)• Personal Directories (PD)• Presence Publisher• IP Media Services

* Required Value.

Save Cancel

On the **Node ID: 1004 - Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **SIP domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, “**avayalab.com**” was used in the shared Avaya Solution and Interoperability Test lab environment. The SIP domain name for the enterprise known to Verizon is “**adevc.avaya.globalipcom.com**”, and the SIP domain will be adapted by the ASBCE for calls to and from the Avaya CS1000E.
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter a descriptive name
- **Application node ID:** Enter “**<Node id>**”. In the sample configuration, Node “**1004**” was used matching the node shown in **Section 5.1**.

The values defined for the sample configuration are shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1004 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avayalab.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: node1004 *

Gateway password: *

Application node ID: 1004 * (0-9999)

Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)
Information will be captured for the IP addresses listed below.

Monitor IP: Add

Monitor addresses: Remove

Scroll down to the **SIP Gateway Settings** → **Proxy or Redirect Server**: section.

Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration, “10.80.150.206” was used.
- **Port:** Enter “5060”.
- **Transport protocol:** Select “TCP”.

The values defined for the sample configuration are shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1004 - Virtual Trunk Gateway Configuration Details

[General](#) | [SIP Gateway Settings](#) | [SIP Gateway Services](#)

Proxy Server Route 1:

Primary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

Transport protocol:

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

Transport protocol:

Scroll down and repeat these steps for the **Proxy Server Route 2** (not shown).

Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. In general, the **SIP URI Map** values have been set to blank for calls that may ultimately be routed to the Verizon IP Trunk service. The Avaya CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the P-Asserted-Identity. If the value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

Node ID: 1004 - Virtual Trunk Gateway Configuration Details	
General <u>SIP Gateway Settings</u> SIP Gateway Services	
SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: <input type="text"/>	CDP: <input type="text"/>
Special number: <input type="text"/>	Special number: <input type="text"/>
Unknown: <input type="text"/>	Vacant number: <input type="text"/>
	Unknown: <input type="text"/>

Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen. Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.

Managing: 10.80.141.202 Username: admin2	
System » IP Network » <u>IP Telephony Nodes</u> » Node Saved	
Node Saved	
Node ID: 1004 has been saved on the call server.	
The new configuration must also be transferred to associated servers and media cards.	
Transfer Now...	You will be given an option to select individual servers, or transfer to all.
Show Nodes	You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

<input type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/>	vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

Select the check box associated with the appropriate Hostname and click **Start Sync**.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown in the previous screen) to **Synchronized** (as shown below). After synchronization completes, select the check box associated with the appropriate Hostname and click **Restart Applications**.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

5.4. Routing of Dialed Numbers to Session Manager

This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Verizon IP Trunk service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a CS1000E telephone user to dial 9-1-303-538-7022 to reach a PSTN telephone using the Verizon IP Trunk service. Other routing policies may be appropriate for different customer networks.

5.4.1 Route List Block

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - **Route List Block (RLB)**
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)

The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click to **Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index 15 is used.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (0 - 1999)

⌘ **Route List Block Index -- 15**

If adding the route list index anew, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate **Data Entry Index** as shown below, and scroll down to the **Options** area of the screen.

+ **Data Entry Index -- 0** **Edit**

Under the **Options** section, select “<**Route id**>” in the **Route Number** field. In the sample configuration route number 15 was used. Default values may be retained for remaining fields as shown below.

Indexes	
Time of Day Schedule:	0 ▼
Facility Restriction Level:	0 (0 - 7)
Digit Manipulation Index:	0 ▼
ISL D-Channel Down Digit Manipulation Index:	0 (0 - 1999)
Free Calling Area Screening Index:	0 ▼
Free Special Number Screening Index:	0 ▼
Business Network Extension Route:	<input type="checkbox"/>
Incoming CLID Table:	0 (0 - 1)
Options	
Local Termination entry:	<input type="checkbox"/>
Route Number:	15 ▼
Skip Conventional Signaling:	<input type="checkbox"/>

Click **Save** (not shown) to save the Route List Block definition.

5.4.2 NARS Access Code

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.4.1**. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit “9” was used.

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 9

NARS Access Code 2:

NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☒

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: 6 (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

- Maximum number of Steering Codes: 2000 (1 - 64000)

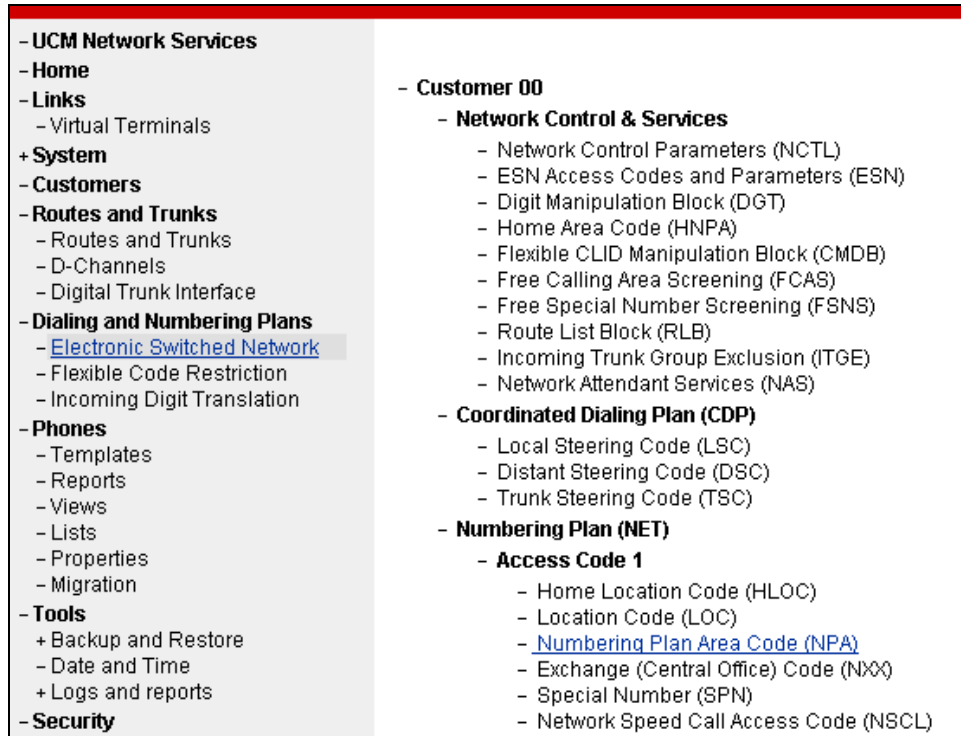
- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3 - 10)

Routing Controls: ☐

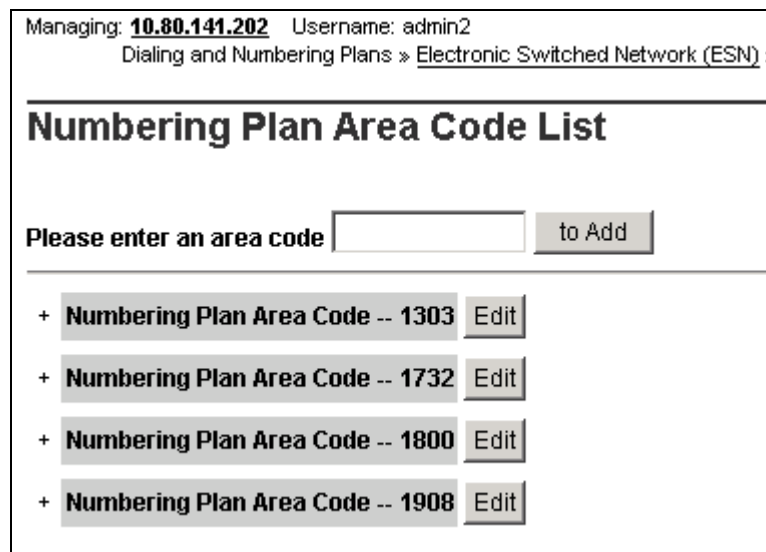
Check for Trunk Group Access Restrictions: ☐

5.4.3 Numbering Plan Area Codes

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as 1800 and 1303 are configured.



In the screen below, the entry for “1303” is displayed. In the Route List Index, “15” is selected to use the route list associated with the SIP Trunk to Session Manager. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Session Manager.

Numbering Plan Area Code

General Properties

Numbering Plan Area code translation:

Route List Index:

Incoming Trunk group Exclusion Index:

5.4.4 Other Special Numbers to Route to Session Manager

In the testing associated with these Application Notes, non-emergency service numbers such as x11, 1x11, international calls, and operator assisted calls were also routed to Session Manager and ultimately to the Verizon IP Trunk service. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.4.3**).

Add a new number by entering it in the **Please enter a Special Number** box and click to **Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as 0, 011, and non-emergency x11 calls are listed. In each case, **Route list index** “15” has been selected in the same manner as shown for the NPAs in the prior section. For special numbers, the **Flexible length** field can also be configured as appropriate for the number. For example, for 511, the **Flexible length** field can be set to 3.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) »

Special Number List

Please enter a Special Number

+ **Special Number -- 0**
+ **Special Number -- 011**
+ **Special Number -- 0144**
+ **Special Number -- 1411**
+ **Special Number -- 311**
+ **Special Number -- 411**
+ **Special Number -- 511**
+ **Special Number -- 711**

5.5. Zones

Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System** → **IP Network** and select **Zones** as shown below.

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- [Zones](#)

Managing: **10.80.141.202** Username: admin2
System » IP Network » Zones

Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones
Numbering zones are used to route calls through a centralized call server.

Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured as shown below. In production environments, it is likely that more zones will be required, Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is Zone number 99.

Managing: **10.80.141.202** Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete Refresh

	Zone ▲	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	<input type="radio"/> 1	1000000	BQ	1000000	BQ	SHARED	MO	IPSETS
2	<input type="radio"/> 99	1000000	BB	1000000	BB	SHARED	VTRK	VTRUNK

In the resultant screen shown below, select **Zone Basic Property and Bandwidth Management**.

Managing: **10.80.141.202** Username: admin2
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 99 » Edit Bandwidth Zone

Edit Bandwidth Zone

- Zone Basic Property and Bandwidth Management
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Time Difference and Daylight Saving Time Property
- Media Services Zone Properties

The following screen shows the Zone 99 configuration. Note that “**Best Bandwidth (BB)**” is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with Verizon IP Trunk service.

Managing: **10.80.141.202** Username: admin2
 System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 99 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	99 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB) ▼
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	VTRUNK

5.6. Codec Parameters, Including Ensuring Annexb=no for G.729

Verizon IP Trunk Service does not support G.729 Annex B, and Verizon requires that SDP offers and SDP answers in SIP messages include the “annexb=no” attribute when G.729 is used. This section includes the configuration that determines whether the “annexb=no” attribute is included.

5.6.1 Media Gateway Configuration

To ensure that the “annexb=no” attribute is included, expand **System** → **IP Network** on the left panel and select **Media Gateways**. Select the appropriate media gateway (not shown), and scroll down to the area of the screen containing **VGW and IP phone codec profile** as shown below.

- UCM Network Services

- Home
- Links
 - Virtual Terminals
- **System**
 - + Alarms
 - + Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - **Media Gateways**
 - Zones
 - Host and Route Tables
 - Network Address Translation
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Software
- **Customers**
- **Routes and Trunks**
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- **Dialing and Numbering Plans**
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- **Phones**

- Media Gateway (MGS)

Hostname

Embedded LAN (ELAN) IP address

Embedded LAN (ELAN) gateway IP address

Embedded LAN (ELAN) subnet mask

Telephony LAN (TLAN) IP address

Telephony LAN (TLAN) gateway IP address

Telephony LAN (TLAN) subnet mask

- DSP Daughterboard

Type of the DSP daughterboard

Telephony LAN (TLAN) IP address

Telephony LAN (TLAN) gateway IP address

Telephony LAN (TLAN) IPv6 address

Telephony LAN (TLAN) subnet mask

Hostname

✖ VGW and IP phone codec profile

+ QoS

+ Media Based CLID

- Call Server LAN

Expand **VGW and IP phone codec profile**. To use G.729A with Verizon IP Trunk service, ensure that the **Select** box is checked for **Codec G729A**, and the **VAD** (Voice Activity Detection) box is un-checked.

Note that **Codec G.711** is enabled by default. **Voice payload size** “20” can be used with Verizon IP Trunk service for both G.729A and G.711. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. The following screen shows the parameters used.

The screenshot displays two codec configuration sections. The top section is for **- Codec G711**, which has its **Select** checkbox checked. Below it, the **Codec name** is G711, **Voice payload size** is 20 (ms/frame), **Voice playout (jitter buffer) nominal delay** is 40, and **Voice playout (jitter buffer) maximum delay** is 80. A red warning message states: "Modifications may cause changes to dependent settings". The **VAD** checkbox is unchecked. The bottom section is for **- Codec G729A**, which has its **Select** checkbox checked (circled in orange). Below it, the **Codec name** is G729A, **Voice payload size** is 20 (ms/frame), **Voice playout (jitter buffer) nominal delay** is 40, and **Voice playout (jitter buffer) maximum delay** is 80. A red warning message states: "Modifications may cause changes to dependent settings". The **VAD** checkbox is unchecked (circled in orange).

5.6.2 Node Voice Gateway and Codec Configuration

Expand **System** → **IP Network** and select **Node, Server, Media Cards**. Select the appropriate **Node Id** “1004” as shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

<input type="checkbox"/> Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 1004	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.203		Synchronized

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

In the resultant screen (not shown) use the scroll bar on the right to select **Voice Gateway (VGW) and Codecs**. The following screen shows the **General** parameters used in the sample configuration.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1004 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128
☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection
☐ Low latency mode
☒ Remove DTMF delay (squelch DTMF from TDM to IP)
☒ Modem/Fax pass-through
☒ V.21 Fax tone detection
☐ R factor calculation

Use the scroll bar on the right to find the area with heading **Voice Codecs**. Note that **Codec G.711** is enabled by default. The following screen shows the G.711 parameters used in the sample configuration.

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked, as shown below. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1004 - Voice Gateway (VGW) and Codecs

General | **Voice Codescs** | Fax

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

5.7. Enabling Plug-Ins for Call Transfer Scenarios

Plug-ins allow specific CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, two plug-ins were enabled as shown in this section.

To view or enable a plug-in, from the left navigation menu, expand **System** → **Software**, and select **Plug-ins**. In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in 501 is displayed as shown in the screen below. If the **Status** is “Disabled”, select the check-box next to Number 501 and click the **Enable** button at the top, if it is desirable to allow CS1000E users to complete call transfer to PSTN destinations via the Verizon IP Trunk service before the call has been answered by the PSTN user. Note that enabling Plug-in 501 will allow the user to complete the transfer while the call is in a ringing state, but no audible ring back tone will be heard after the transfer is completed.

AVAYA CS1000 Element Manager				
- System + Alarms - Maintenance + Core Equipment - Peripheral Equipment - IP Network - Nodes: Servers, Media Cards - Maintenance and Reports - Media Gateways - Zones - Host and Route Tables - Network Address Translation (NAT) - QoS Thresholds - Personal Directories - Unicode Name Directory + Interfaces + Engineered Values + Emergency Services - Software - Call Server PEPs - Loadware PEPs - File Upload - IP Phone Firmware - Voice Gateway Media Card - Media Cards PEPs - Plug-ins - Customers	<input type="button" value="Enable"/> <input type="button" value="Disable"/>			
	<input type="checkbox"/>	Number	Description	MPLR Number
	<input type="checkbox"/>	222	PI: Remote secondary dialtone after user dial #000000	MPLR222000
	<input type="checkbox"/>	223	PI: HICOM REJECTS QSIG CCBS REQUEST WITH NO CALLING NUMBER	MPLR12290
	<input type="checkbox"/>	224	PI: No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676
	<input type="checkbox"/>	225	PI: PKG 179, Taurus, electronic look, Mail and CallPilot softkeys	MPLR22389
	<input type="checkbox"/>	226	PI: ACLID should display more than 10 digits	MPLR15783
	<input type="checkbox"/>	228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613
	<input type="checkbox"/>	230	PI: Unplugged telset disables after midnight routines.	MPLR11700
	<input type="checkbox"/>	231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878
	<input type="checkbox"/>	232	PI: QSIG GF: No diverting and originally called number in DL12 APDU on calls from MCDN TRO-BA.	MPLR24273
	<input type="checkbox"/>	233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506
	<input type="checkbox"/>	235	Restrict Hands-free functionality for all IP set types.	MPLR29100
	<input type="checkbox"/>	500	NO DESCRIPTION	MPLR21979
	<input type="checkbox"/>	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070
	<input type="checkbox"/>	504	PRI232 BUG253 from PI 10 Delay in Response at Called IFC	MPLR24744
	<input type="checkbox"/>	505	UM2K integration problem with S100 Interface	MPLR30004

The same procedure may be used to enable Plug-in 201 if desired. Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IP Trunk service, and then subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IP Trunk service.

5.8. Customer Information

This section documents basic Customer configuration relevant to the sample configuration. This section is not intended to be prescriptive. Select **Customers** from the left navigation menu, click on the appropriate **Customer Number** and select **ISDN and ESN Networking** (not shown). The following screen shows the **General Properties** used in the sample configuration.

Managing: **10.80.141.202** Username: admin2
Customers » Customer 00 » Customer Details » ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code: (0 - 9999)
Code for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks
☒ Connection of supervised external trunks

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-DID users: ☒ Coordinated dialing plan
☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Size: (0 - 4000)

Country code: (0 - 9999)
Code displayed as part of calling number

[Calling Line Identification Entries](#)

5.8.1 Caller ID Related Configuration

Although not intended to be prescriptive, in the sample configuration the CS1000E would send the user's four-digit directory number in SIP headers such as the From and PAI headers. Session Manager would adapt the user's directory number to an appropriate Verizon IP Trunk DID number before passing the message to the ASBCE towards Verizon.

Scroll down from the screen shown in **Section 5.8**, click the **Calling Line Identification Entries** link (now shown), and search for the **Calling Line Identification Entries** by **Entry ID**. As shown below, the **Use DN as DID** parameter was set to **"NO"** and an entry ID was created for every DID used in the sample configuration. The local DID will be replaced with the **Local Code** and the **Entry ID** will be configured on the individual extensions in **Section 5.9**.

Managing: **10.80.141.202** Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range :
End range :
'End range' should not exceed the CLID size specified

Calling Line Identification Entries

<input type="checkbox"/>	Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1 <input type="checkbox"/>	0		7329450232			NO	
2 <input type="checkbox"/>	1		7329450231			NO	
3 <input type="checkbox"/>	2		7329450233			NO	
4 <input type="checkbox"/>	3		7329450234			NO	

Click on **Entry Id 0** to view or change further details as shown below.

Managing: **10.80.141.202** Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0

Edit Calling Line Identification 0

General Properties

National Code: (0 - 999999)
Code for national home number

Local Code: (1-12 digits)
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID :

5.8.1.1 Requesting Privacy

One means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IP Trunk service is to set **CLBA Calling Party Privacy** to “**Allowed**” via the Phone **Features** in Element Manager as shown below.

Feature	Description	Status
CDMA	External Station Activity Records	Denied
CFHA	Call Forward/Hunt Override	Denied
CFTA	Call Forward by Call Type	Denied
CFXA	Call Forward External	Denied
CLBA	Calling Party Privacy	Allowed

Another means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IP Trunk service is to set **DDGA Present/Restrict Calling Number** to “**Denied**” via the Phone **Features** in Element Manager (not shown).

5.9. Example CS1000E Telephone Users

This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration.


5.9.1 Example IP UNISTim Phone DN 2000, Codec Considerations

The following screen shows basic information for an IP UNISTim phone in the configuration. The telephone is configured as Directory Number 2000. Note that the telephone is in Zone 1. A call between this telephone and another telephone in Zone 1 will use a “best quality” strategy (see **Section 5.5**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IP Trunk service, the call would use a “best bandwidth” strategy, and the call would use G.729A.

The screenshot displays the Avaya configuration interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Phones' category is selected. The main area shows 'Managing: EM on vz-cs1k(10.80.141.202)' and a link to 'Phones»Phone Details'. Below this is the 'Phone Details' section, which includes an image of a telephone and the following information: System: EM on vz-cs1k, Phone Type: 1165, and Sync Status: TRN. A tabbed interface below shows 'General Properties' selected, with other tabs for Features, Keys, and User Fields. The 'General Properties' section contains fields for Customer Number (0), Terminal Number (252 0 00 00), Designation (IPSET), and Zone (1).

Managing: [EM on vz-cs1k\(10.80.141.202\)](#)
[Phones»Phone Details](#)

Phone Details



System: EM on vz-cs1k
Phone Type: 1165
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Zone: *

Scrolling down to the **Keys** section. The **First** and **Last Name**, the **Directory Number** as well as the **Calling Lined ID (CLID)** is configured. The **CLID** entry is defined in **Section 5.8.1**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, and Phones. The main content area is titled 'Keys' and displays a table with columns 'Key No.', 'Key Type', and 'Key Value'. A single entry is shown with 'Key No.' 0 and 'Key Type' 'SCR - Single Call Ringing'. To the right of the table, there are configuration fields: 'Directory Number' set to 2000, a checked box for 'Multiple Appearance Redirection Prime(MARP)', and fields for 'First Name' (1165), 'Last Name' (UNISTIM), 'Display Format' (First, Last), and 'Language' (Roman). At the bottom, there is a 'CLID Entry (Numeric or D)' field set to 0 and an 'ANIE Entry' field.

5.9.2 Example SIP Phone DN 2900, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 2900. Note that the telephone is in Zone 1 and is associated with Node 1004 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use a “best quality” strategy (see **Section 5.5**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IP Trunk service, the call would use a “best bandwidth” strategy, and the call would use G.729A.

The screenshot shows the AVAYA CS1000 Element Manager interface for a SIP phone configuration. The left sidebar is the same as the previous screenshot. The main content area is titled 'General Properties' and displays various configuration fields. At the top, there is a phone icon and system information: 'System: EM on vz-cs1k', 'Phone Type: UEXT-SIPL', and 'Sync Status: TRN'. Below this, there are tabs for 'General Properties', 'Features', 'Keys', and 'User Fields'. The 'General Properties' tab is active, showing fields for 'Customer Number' (0), 'Terminal Number' (252 0 09 00), 'Designation' (SIPN), 'Zone' (1), 'SIP User Name' (2900), and 'Node Id' (1004). Each field has a star icon indicating it is required.


5.9.3 Example Digital Phone DN 2222

The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 2222.

The screenshot shows a web-based configuration interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Phones' category is selected. The main content area is titled 'Phone Details' and shows information for a phone managed by 'EM on vz-cs1k(10.80.141.202)'. It includes a photo of a phone and fields for System, Phone Type, and Sync Status. Below this are tabs for General Properties, Features, Keys, and User Fields. The 'General Properties' tab is active, showing fields for Customer Number, Terminal Number, and Designation.

Managing: **EM on vz-cs1k(10.80.141.202)**
[Phones»Phone Details](#)

Phone Details

 System: EM on vz-cs1k
Phone Type: M3904
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone, and uses **CLID Entry 1 (Section 5.8.1)**. Although not shown in detail below, to use call waiting with tone, assign a key “CWT – Call Waiting”, set the feature “SWA – Call waiting from a Station” to “Allowed”, and set the feature “WTA – Warning Tone” to “Allowed”.

The screenshot shows the 'Keys' configuration page. It has a table with columns 'Key No.', 'Key Type', and 'Key Value'. The first row shows Key No. 0, Key Type 'SCR - Single Call Ringing', and Key Value '2222'. Below the table are various configuration options for the key, including a checkbox for 'Multiple Appearance Redirection Prime(MARP)', fields for 'First Name', 'Last Name', 'Display Format', and 'Language', and fields for 'CLID Entry (Numeric or D)' and 'ANIE Entry'.

Keys

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	2222

☒ Multiple Appearance Redirection Prime(MARP)

First Name: Last Name: Display Format: Language:

CLID Entry (Numeric or D):

ANIE Entry:

5.9.4 Example Analog Port with DN 2221, Fax

The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine. The port is configured as **Directory Number 2221** with **CLID entry 3**.

System: EM on vz-cs1k
Phone Type: 500
Sync Status: TRN

[General Properties](#) | [Features](#) | [Single Line Features](#) | [User Fields](#)

General Properties

Customer Number: 0 *

Terminal Number: 004 0 04 00

Designation: Analog * (1-6 characters)

Directory Number: 2221 *

CLID entry: 3

ANIE entry:

Marp ☒

When an analog port is used for a fax call, the call may start out using codec G.729A. However, once fax tone is heard, the codec in use will automatically renegotiate to G.711MU for “fax over G.711MU”, assuming T.38 is not yet available in the Verizon network, as was the case on the production circuit used for the testing associated with these Application Notes.

5.10. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** for **Action** and click **Submit** to save configuration changes as shown below.

The screenshot displays the Avaya Communication Server 1000E web interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore', 'Call Server' (highlighted), and 'Personal Directories'. The main content area is titled 'Call Server Backup'. At the top, it shows 'Managing: 10.80.141.202' and 'Username: admin2'. Below this is a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The main heading is 'Call Server Backup'. Underneath, there is an 'Action' label followed by a dropdown menu set to 'Backup', and two buttons: 'Submit' and 'Cancel'.

The backup process may take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
Backing up reten.bkp
Starting database backup
to local Removable Media Device
USB mass storage device found available
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/usb/backup/single"
Database backup Complete!
TEMU207
Backup process to local Removable Media Device ended successfully.
```

The configuration of Avaya Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in Section 11.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP trunk between Session Manager and the ASBCE.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “<http://<ip-address>/SMGR>”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button.

AVAYA Avaya Aura® System Manager 6.1

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

User ID:

Password:

[Change Password](#)

Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.

Users	Elements	Services
Administrators Manage Administrative Users Groups & Roles Manage groups, roles and assign roles to users Subscribers Manage users and shared resources associated with CS1000, including LDAP/file import and export Synchronize and Import Synchronize users with the enterprise directory, import users from file UCM Roles Manage UCM Roles, assign roles to users User Management Manage users, shared user resources and provision users	Application Management Manage applications and application certificates Communication Manager Manage Communication Manager objects Conferencing Conferencing Inventory Manage, discover, and navigate to elements, update element software Messaging Manage Messaging System objects Presence Presence Routing Network Routing Policy Session Manager Session Manager Element Manager SIP AS 8.1 SIP AS 8.1	Backup and Restore Backup and restore System Manager database Configurations Manage system wide configurations Events Manage alarms, view and harvest logs Licenses View and configure licenses Replication Track data replication nodes, repair replication nodes Scheduler Schedule, track, cancel, update and delete jobs Security Manage Security Certificates Templates Manage Templates for Communication Manager and Messaging System objects UCM Services Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

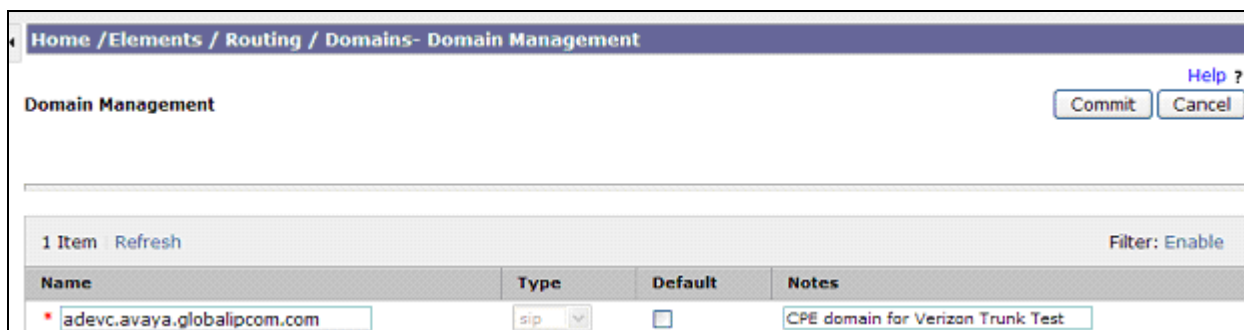
▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

6.1. SIP Domain

Select **Domains** from the left navigation menu. Two domains can be added, one for the enterprise SIP domain, and one for the Verizon network SIP domain. In the shared environment of the Avaya Solution and Interoperability Test lab, a domain “avayalab.com” is also defined and used by the shared equipment.

Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, “**adevc.avaya.globalipcom.com**” is shown, the CPE domain known to Verizon.
- **Type:** Verify “**SIP**” is selected.
- **Notes:** Add a brief description. [Optional].



Home / Elements / Routing / Domains- Domain Management

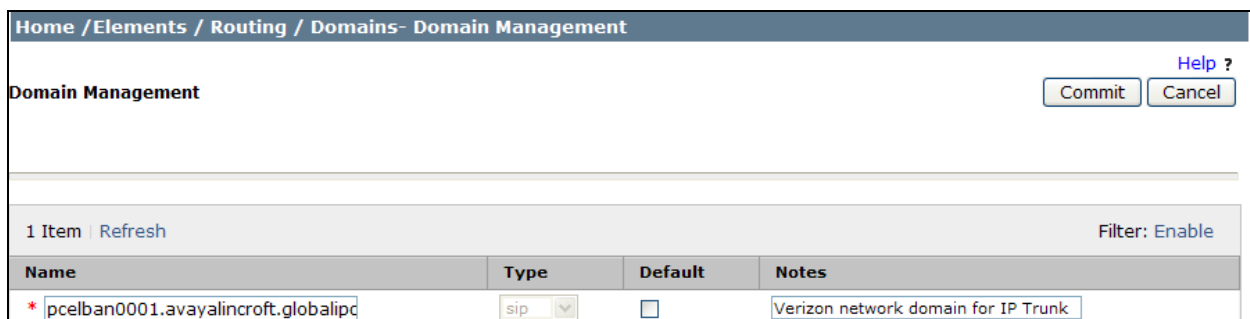
Domain Management [Help ?](#)

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Trunk Test

Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name:** Enter the Domain Name used for the Verizon network. In the sample screen below, “**pcelban0001.avayalincroft.globalipcom.com**” is shown.
- **Type:** Verify “**SIP**” is selected.
- **Notes:** Add a brief description. [Optional].



Home / Elements / Routing / Domains- Domain Management

Domain Management [Help ?](#)

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk

Click **Commit** to save.

The following screen shows the “**avayalab.com**” SIP domain that was already configured in the shared laboratory network.

Home / Elements / Routing / Domains - Domain Management

Domain Management

1 Item Refresh

Name	Type	Default	Notes
* avayalab.com	sip	<input type="checkbox"/>	Shared Avaya SIL network

The screen below shows an example SIP Domain list after SIP Domains are configured. Many SIP Domains can be configured, distinguished, and adapted by the same Session Manager as needed.

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions ▾

7 Items Refresh

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Test Trunk
<input type="checkbox"/>	attaep60.com	sip	<input type="checkbox"/>	Testing with AEP6.0
<input type="checkbox"/>	attavaya.com	sip	<input type="checkbox"/>	Testing ATT VP
<input type="checkbox"/>	avayalab.com	sip	<input type="checkbox"/>	Shared Avaya SIL network
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk
<input type="checkbox"/>	qwest.com	sip	<input type="checkbox"/>	Qwest SIP Trunk
<input type="checkbox"/>	sip.avaya.com	sip	<input type="checkbox"/>	

Select : All, None

6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be used for bandwidth management or location-based routing.

6.2.1 Location for Avaya Communication Server 1000E

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Click **Commit** to save. **Note:** No IP Address is added in the **Location Pattern** section.

The screen below shows the top portion of the screen for the Location defined for Avaya Communication Server 1000E.

Home / Elements / Routing / Locations - Location Details

Location Details [Help ?](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

0 Items | [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

* Input Required

6.2.2 Location for Avaya SBC For Enterprise

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Click **Commit** to save.

The screen below shows the Location defined for the ASBCE.

[Home](#) / [Elements](#) / [Routing](#) / [Locations - Location Details](#)

Location Details

[Help ?](#)

CommitCancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

ASBCE_1_Loc_140

Notes:

10.80.140.140

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

AddRemove

0 Items

[Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

* Input Required

CommitCancel

6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent to Avaya Communication Server 1000E to the format used by other Avaya products and endpoints.

6.3.1 Adaptation for Avaya Communication Server 1000E

Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., “Vz_CS1K7.5”).
- **Module Name:** Select “CS1000Adapter” from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined).

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details [Help ?](#)

[Commit](#) [Cancel](#)

General

* Adaptation name: Vz_CS1K7.5

Module name: CS1000Adapter

Module parameter:

Egress URI Parameters:

Notes:

Scrolling down, in the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from Verizon to CS1000E users. The text below and the screen example that follows explain how to use Session Manager to convert between Verizon DID numbers and corresponding CS1000E directory numbers. **Digit Conversion for Incoming Calls to SM** could be used, however the extensions will be adapted by the CLID entries on the individual extensions (**Section 5.9**).

- **Matching Pattern** Enter Verizon DID numbers (or number ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min** Enter minimum number of digits (e.g., 10).
- **Max** Enter maximum number of digits (e.g., 10).
- **Delete Digits** Enter “10”, the number of digits to be removed from dialed DID number before routing by Session Manager. For Verizon DID conversion to the corresponding CS1000E extension, remove all digits in the DID number.
- **Insert Digits** Enter the CS1000E extension corresponding to the DID number.
- **Address to modify** Select “both”.

Digit Conversion for Incoming Calls to SM

Add Remove
0 Items Refresh
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
Digit Conversion for Outgoing Calls from SM								
Add Remove 4 Items Refresh Filter: Enable								
	Matching Pattern ^	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	2222	both	
<input type="checkbox"/>	* 7329450232	* 10	* 10		* 10	2000	both	
<input type="checkbox"/>	* 7329450233	* 10	* 10		* 10	2900	both	
<input type="checkbox"/>	* 7329450234	* 10	* 10		* 10	2221	both	

Select : All, None

Click **Commit**.

6.3.2 Adaptation for Avaya SBC for Enterprise

Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module.
- **Module Name:** Select “**VerizonAdapter**” from drop-down menu (or add an adapter with name “VerizonAdapter” if not previously defined).
- **Module Parameter:** Enter “**MIME=no**” to strip the CS1000E MIME information from the SDP sent to Verizon.

The screenshot shows the 'Adaptation Details' configuration page in the Avaya SBC GUI. The breadcrumb trail at the top is 'Home / Elements / Routing / Adaptations - Adaptation Details'. The page has a 'Commit' and 'Cancel' button in the top right corner. The 'General' section contains the following fields: 'Adaptation name' (text input with value 'History Diversion IPT'), 'Module name' (dropdown menu with 'VerizonAdapter' selected), 'Module parameter' (text input with value 'MIME=no'), 'Egress URI Parameters' (text input), and 'Notes' (text input). Below this is the 'Digit Conversion for Incoming Calls to SM' section, which includes 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' link. The table has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, and Notes. Below this is the 'Digit Conversion for Outgoing Calls from SM' section, which also includes 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' link. The table has the same columns as the one above. At the bottom of the page, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

Commit Cancel

General

* Adaptation name: History Diversion IPT

Module name: VerizonAdapter

Module parameter: MIME=no

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

* Input Required

Commit Cancel

Click **Commit**.

6.4. SIP Entities

SIP Entities must be added for Avaya Communication Server 1000E and for the ASBCE.

6.4.1 SIP Entity for Avaya Communication Server 1000E

Select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity.
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E Node.
- **Type:** Select “**SIP Trunk**”.
- **Notes:** Enter a brief description. [Optional].
- **Adaptation:** Select the Adaptation Module for CS1000E created in **Section 6.3.1**.
- **Location:** Select the Location for CS1000E.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**” (or choose an alternate Link Monitoring approach for this entity, if desired).

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Avaya Communication Server 1000E in the sample configuration.

The screenshot displays the 'SIP Entity Details' configuration window. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The window title is 'SIP Entity Details'. In the top right corner, there are 'Commit', 'Cancel', and 'Help ?' buttons. The 'General' section is active, showing the following fields:

- Name:** Vz_CS1K_7.5
- FQDN or IP Address:** 10.80.140.203
- Type:** SIP Trunk (dropdown menu)
- Notes:** CS1000E 7.5
- Adaptation:** Vz_CS1K7.5 (dropdown menu)
- Location:** Vz_CS1K (dropdown menu)
- Time Zone:** America/Denver (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

6.4.2 SIP Entity for Avaya SBC for Enterprise

Select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity.
- **FQDN or IP Address:** Enter the private side IP Address of the SBC.
- **Type:** Select “**Other**”.
- **Notes:** Enter a brief description. [Optional].
- **Adaptation:** Select the Adaptation Module for the ASBCE created in **Section 6.3.2**.
- **Location:** Select the Location for the ASBCE.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**” (or choose an alternate Link Monitoring approach for this entity, if desired).

The following screen shows the SIP Entity defined for the ASBCE in the sample configuration.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details Help ? Commit Cancel

General

* Name: Vz_ASBCE-1

* FQDN or IP Address: 10.80.140.141

Type: Other

Notes:

Adaptation: History Diversion IPT

Location: ASBCE_1_Loc_140

Time Zone: America/Denver

Override Port & Transport with DNS ☐

SRV:

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 5

6.5. Entity Links

The SIP trunk between Session Manager and Avaya Communication Server 1000E is described by an Entity Link, as is the SIP trunk between Session Manager and the ASBCE.

6.5.1 Entity Link to Avaya Communication Server 1000E

Select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name:** Enter an identifier for the link.
- **SIP Entity 1:** Select SIP Entity defined for Session Manager.
- **Protocol:** Select protocol to use “TCP”.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is “5060”.
- **SIP Entity 2:** Select the SIP Entity defined for CS1000E.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is “5060”.
- **Trusted** Check this option box.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save the **Entity Link** definition.

The following screen shows the Entity Link defined for the SIP trunk between Session Manager and Avaya Communication Server 1000E.

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Vz_CS100075-Link	* ASM	TCP	* 5060	* Vz_CS1K_7.5	* 5060	Trusted	

6.5.2 Entity Link to Avaya SBC for Enterprise

Select **Entity Links** from the left navigation menu. Click **New** (not shown). Enter the following values.

- **Name:** Enter an identifier for the link.
- **SIP Entity 1:** Select SIP Entity defined for Session Manager.
- **SIP Entity 2:** Select the SIP Entity defined for the ASBCE.
- **Protocol:** After selecting both SIP Entities, select “TCP”.
- **Port:** Verify **Port** for both SIP entities is the default listen port.
For the sample configuration, default listen port is “5060”.
- **Trusted:** Check this option box.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and the SBC.

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Vz_ASM_ASBCE-1	* ASM	TCP	* 5060	* Vz_ASBCE-1	* 5060	Trusted	

6.6. Routing Policies

Routing Policies describe the conditions under which calls will be routed to the Avaya Communication Server 1000E or the ASBCE.

6.6.1 Routing Policy to Avaya Communication Server 1000E

To add a new Routing Policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values:

- **Name:** Enter an identifier to define the Routing Policy.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with CS1000E and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for Avaya Communication Server 1000E.

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details Commit Cancel [Help ?](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Vz_CS1K_7.5	10.80.140.203	SIP Trunk	CS1000E 7.5

6.6.2 Routing Policy to Avaya SBC for Enterprise

To add a new Routing Policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the Routing Policy.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the ASBCE and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the ASBCE.

The screenshot shows the 'Routing Policy Details' page for 'Vz_ASBCE-1_RP'. The page has a breadcrumb trail: 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. There are 'Commit', 'Cancel', and 'Help' buttons in the top right. The 'General' section contains fields for 'Name' (Vz_ASBCE-1_RP), 'Disabled' (checkbox), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button. Below is a table with columns: Name, FQDN or IP Address, Type, and Notes.

Name	FQDN or IP Address	Type	Notes
Vz_ASBCE-1	10.80.140.141	Other	

6.7. Dial Patterns

Dial Patterns are used to route calls to the appropriate Routing Policies, and ultimately to the appropriate SIP Entities. Dial Patterns will be configured to route outbound calls from CS1000E users to the PSTN via the Verizon IP Trunk Service. Other dial patterns will be configured to route inbound calls from Verizon IP Trunk Service to CS1000E users.

6.7.1 Inbound Verizon Calls to CS1000E Users

To define a Dial Pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E (e.g., a Verizon DID number).
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**” or alternatively, select a specific Location (e.g. “**ASBCE_1_Loc_140**”). In the example below, the ASBCE Location was selected as the originating Location.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E (“**Vz_CS1K_7.5**”).
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save.

The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional Verizon DID numbers to be routed to the CS1000E. Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details
Help ?
Commit
Cancel

General

* Pattern: 732

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	ASBCE_1_Loc_140	10.80.140.140	Vz_CS1K-R75_RP	0	<input type="checkbox"/>	Vz_CS1K_7.5	

6.7.2 Outbound Calls to Verizon

To define a Dial Pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls destined for the Verizon network.
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “**All**” if Session Manager should route outgoing calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**” or alternatively, select a specific originating Location. In the **Routing Policies** table, select the Routing Policy defined for the ASBCE.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save.

The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional PSTN numbers to be routed to the Verizon network via the ASBCE. Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns - Dial Pattern Details](#)

Dial Pattern DetailsHelp ?
Commit Cancel

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name ¹ ▲	Originating Location Notes	Routing Policy Name	Rank ² ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Vz_CS1K	10.80.140.203	Vz_ASBCE-1_RP	0	<input type="checkbox"/>	Vz_ASBCE-1	

Select : [All](#), [None](#)

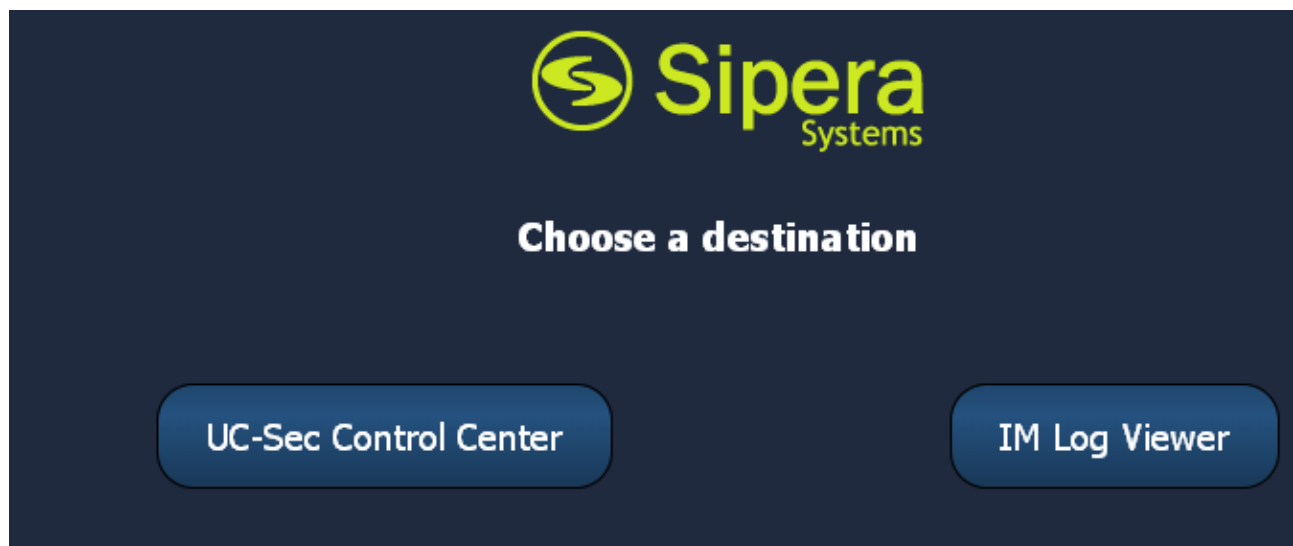
7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya Session Border Controller for Enterprise is used as the edge device between the Avaya CPE and Verizon Business.

These Application Notes assume that the installation of the ASBCE and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

Access the web management interface by entering the URL `https://<ip-address>` where `<ip-address>` is the management IP address assigned during installation. Select **UC-Sec Control Center**.



A log-in screen is presented. Enter an appropriate **Login ID** and **Password**.

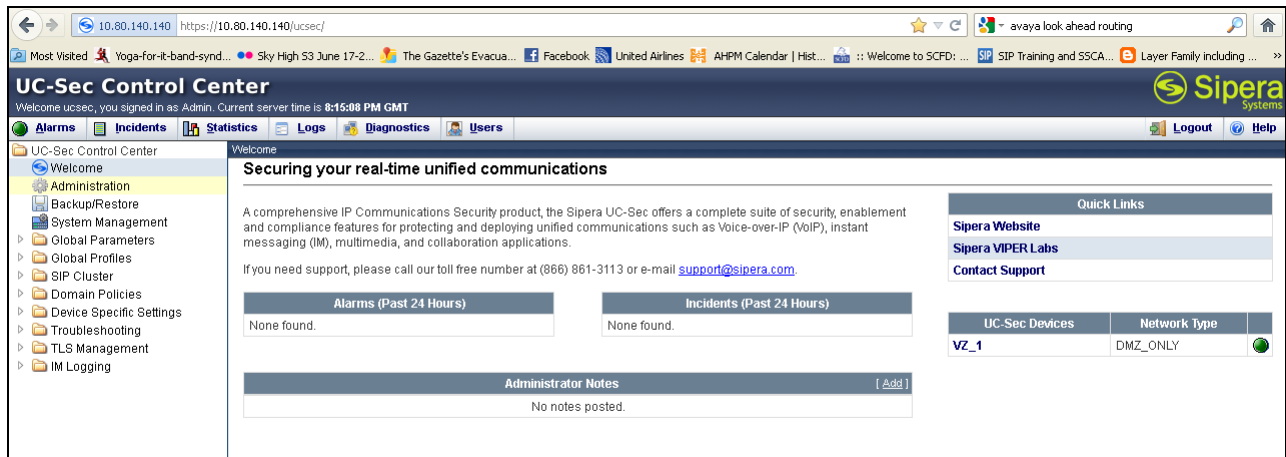


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

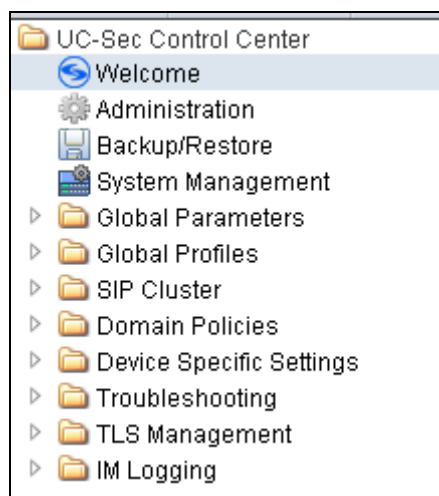
[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

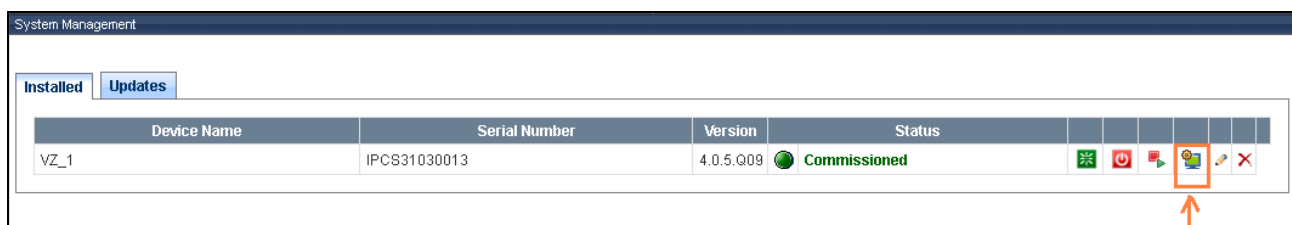
Once logged in, the main page of the UC-Sec Control Center will appear.



The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named VZ_1 is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.

System Information: VZ_1

Network Configuration

General Settings

Appliance Name	VZ_1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.80.140.141	10.80.140.141	255.255.255.0	10.80.140.1	A1
2.2.2.2	2.2.2.2	255.255.255.0	2.2.2.1	B1

DNS Configuration

Primary DNS	172.30.209.4
Secondary DNS	
DNS Location	DMZ
DNS Client IP	2.2.2.2

Management IP(s)

IP	10.80.140.140
----	---------------

7.2. Device Specific Settings

7.2.1 Define Network Information

Network information is required on the ASBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface for the internal side and the **B1** interface for the external side. Each side of the ASBCE can have only one interface assigned. To define the network information, navigate to **Device Specific Settings** → **Network Management** in the **UC-Sec Control Center** menu on the left hand side and click **Add IP**. A new line appears that can be configured.

- **IP Address:** Enter the IP Address for the internal interface.
- **Gateway:** Enter the appropriate gateway IP Address.
- **Interface:** Select the desired hardware interface (**A1**).

Click **Save Changes**. Repeat the process for external interfaces using **B1**.

Note: Multiple IP addresses defined on a single interface must be in the same subnet.

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices

VZ_1

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.0 B2 Netmask

Add IP Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
10.80.140.141		10.80.140.1	A1
2.2.2.2		2.2.2.1	B1

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices

VZ_1

Network Configuration Interface Configuration

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.2.2 Signaling Interfaces

To define the signaling interfaces on the ASBCE, navigate to **Device Specific Settings** → **Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side and Select **Add Signaling Interface**.

Define a signaling interface for Verizon:

- **Name:** Enter a descriptive name for the external signaling interface for the Verizon network.
- **IP Address:** Choose the external address for signaling.
- **TCP/UDP/TLS Port:** Enter the port for the desired protocol.

Click **Finish** (not shown).

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external signaling interfaces used in the sample configuraiton.

Device Specific Settings > Signaling Interface: VZ_1

UC-Sec Devices
VZ_1

Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside_to_CPE	10.80.140.141	5060	5060	---	None		
Sig_Outside_to_Vz	2.2.2.2	---	5060	---	None		

7.2.3 Media Interfaces

To define the media interfaces on the ASBCE, navigate to **Device Specific Settings → Media Interface** in the **UC-Sec Control Center** menu on the left hand side and select **Add Media Interface**. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signaling or can be different.

Define a media interface for Verizon:

- **Name:** Enter a descriptive name for the external media interface for the Verizon network.
- **IP Address:** Choose the external address for the media.
- **Port Range:** Enter port ranges for the media path.

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external media interfaces used in the sample configuraiton.

Device Specific Settings > Media Interface: VZ_1

UC-Sec Devices
VZ_1

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add Media Interface

Name	Media IP	Port Range		
Int_Media_to_CPE	10.80.140.141	35000 - 40000		
Ext_Media_to_Vz	2.2.2.2	35000 - 40000		

7.3. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.3.1 Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Create a Routing Profile for Session Manager and a separate Routing Profile for Verizon SIP Trunk. To add a Routing Profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server with a colon and the port.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server:** Checked.
- **Next Hop in Dialog:** (Optional) Checked only if information in the Via Header is to be used instead of received port and IP.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish** (not shown).

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module followed by a colon and the port being used. The **Outgoing Transport** must match the ASBCE Entity Link created on Session Manager in **Section 6.5**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.80.150.206:5060	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to Verizon. In the **Next Hop Server 1** field enter the IP address that Verizon uses for the IP Trunk with a colon and then the port number. Check the **Next Hop Priority**. Enter **UDP** for the **Outgoing Transport** field.

NOTE: If the outside port is something other than 5060 the “Next Hop Server 1” and “Next Hop Server 2” fields must contain a colon and the port number after the IP address or domain name. If these are not entered, then the OPTIONS messages from Session Manager will be proxied to the service provider with a port of 5060 and may not get a response. This will cause ASBCE to respond to the Session Manager OPTIONS with a 408 Request Timeout, which will cause the Session Manager to mark the entity link as down.

Global Profiles > Routing: Vz_IPT

Add Profile Rename Profile Clone Profile Delete Profile

Routing Profiles

default

Route to SM6.1

Vz_IPCC

Route to SM6.2

Vz_IPT

Click here to add a description.

Routing Profile

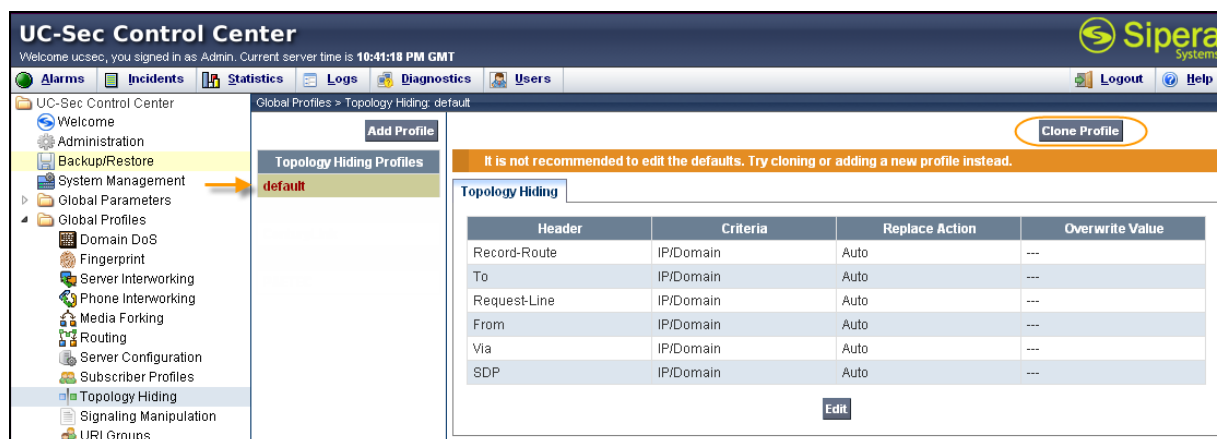
Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	172.30.209.21:5071	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

7.3.2 Topology Hiding Profile

The Topology Hiding Profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Create a Topology Hiding Profile for the enterprise and a separate Topology Hiding Profile for the Verizon SIP Trunk. In the sample configuration, the **Enterprise** and **SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center** → **Global Profiles** → **Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.



Enter a descriptive name for the new profile and click **Finish**.

The 'Clone Profile' dialog box shows the 'Profile Name' as 'default' and the 'Clone Name' as 'Avaya'. The 'Finish' button is highlighted.

Edit the **Avaya** profile to overwrite the **To**, **Request-Line** and **From** headers shown below with the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.1**). Click **Finish** to save the changes.

The 'Edit Topology Hiding Profile' dialog box shows a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	
Request-Line	IP/Domain	Overwrite	avayalab.com
Record-Route	IP/Domain	Auto	
From	IP/Domain	Overwrite	avayalab.com
To	IP/Domain	Overwrite	avayalab.com
Via	IP/Domain	Auto	

The 'Finish' button is highlighted at the bottom.

It is not necessary to modify the **Verizon** profile from the default values if IP addresses are used. The following screen shows the Topology Hiding Policy **Verizon** created for Verizon with the domain names overwritten in the appropriate fields:

Global Profiles > Topology Hiding: Verizon_IPT

Add Profile **Rename Profile** **Clone Profile** **Delete Profile**

Topology Hiding Profiles

- default
- cisco_th_profile
- Avaya
- Verizon_IPT**

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com

Edit

7.3.3 Server Interworking

Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “**Verizon-IPT**” shown below. Click **Next**.

Interworking Profile

Profile Name:

Next

In the new window that appears, default values can be used. Click **Next** to continue.

Editing Profile: Verizon-IPCC	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
Next	

Default values can also be used for the next two windows that appear. Click **Next** to continue.

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
Back Next	

Interworking Profile	
Configuration is not required. All fields are optional.	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]
Back Next	

On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

Click **Finish** to save changes.

Interworking Profile ✖

Advanced Settings

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text" value=""/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Back
Finish

The Avaya profile will be created by cloning the Verizon profile created in the previous section. To clone a Server Interworking Profile for Avaya, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on the previously created profile for the enterprise, then click on **Clone Profile** as shown below.

UC-Sec Control Center Sip
 Welcome ucsec, you signed in as Admin. Current server time is 4:29:16 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout

UC-Sec Control Center
 Welcome
 Administration
 Backup/Restore
 System Management
 Global Parameters
 Global Profiles
 Domain DoS
 Fingerprint
 Server Interworking
 Phone Interworking
 Media Forking
 Routing
 Server Configuration
 Subscriber Profiles
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SIP Cluster
 Domain Policies

Add Profile

Interworking Profiles

cs2100
 avaya-ru
 OCS-Edge-Server
 cisco-ccm
 cups
 Sipera-Halo
 OCS-FrontEnd-Server
 Avaya
 Verizon-IPCC
 Verizon_IPT

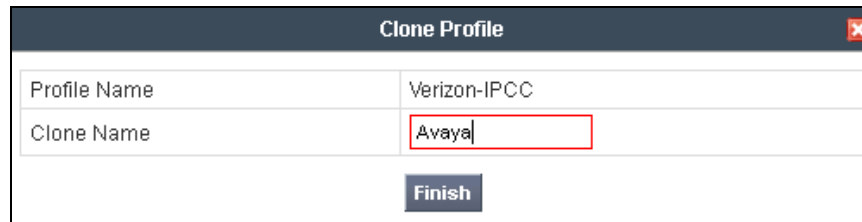
General Timers URI Manipulation Header Manipulation Advanced

General

Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Back
Finish

Enter a descriptive name for the new profile and click **Finish** to save the profile.



Clone Profile	
Profile Name	Verizon-IPCC
Clone Name	Avaya
Finish	

7.3.4 Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the ASBCE. Using this language, a script can be written and tied to a given flow. The ASBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove unwanted headers in the SIP messages to and from Verizon.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. Enter Appropriate script and click **Save**.

The script will act on all outbound traffic to Verizon after the SIP message has been routed through the ASBCE. The script is further broken down as follows:

- **within session “All”** Transformations applied to all SIP sessions.
- **act on message** Actions to be taken to any SIP message.
- **%DIRECTION=“OUTBOUND”** Applied to a message leaving ASBCE.
- **%DIRECTION=“INBOUND”** Applied to a message entering ASBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has routed through ASBCE.
- **%ENTRY_POINT=“PRE_ROUTING”** The “hook point” to apply the script before the SIP message has routed through ASBCE.
- **remove(%HEADERS[“P-Location”][1]);** Used to remove an entire header (like P-Location). The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.

- **%HEADERS["Supported"][1].regex_replace);** Used to find and replace a value in the header. In the screen below, the value "x-nortel-sipvc," found in the header is to be replaced with nothing (""). This method is being used instead of **Remove** because only a portion of the header is being removed.

With this script, the P-Location, Endpoint-View, Alert-Info, x-nt-e164-clid, History-info, User-Agent, and Server headers as well as the "x-nortel-sipvc," text in the Allow header will be removed. These items are being removed for general security purposes and because the SIP Service provider has no need of these items. These are optional inclusions to any SigMa Script.

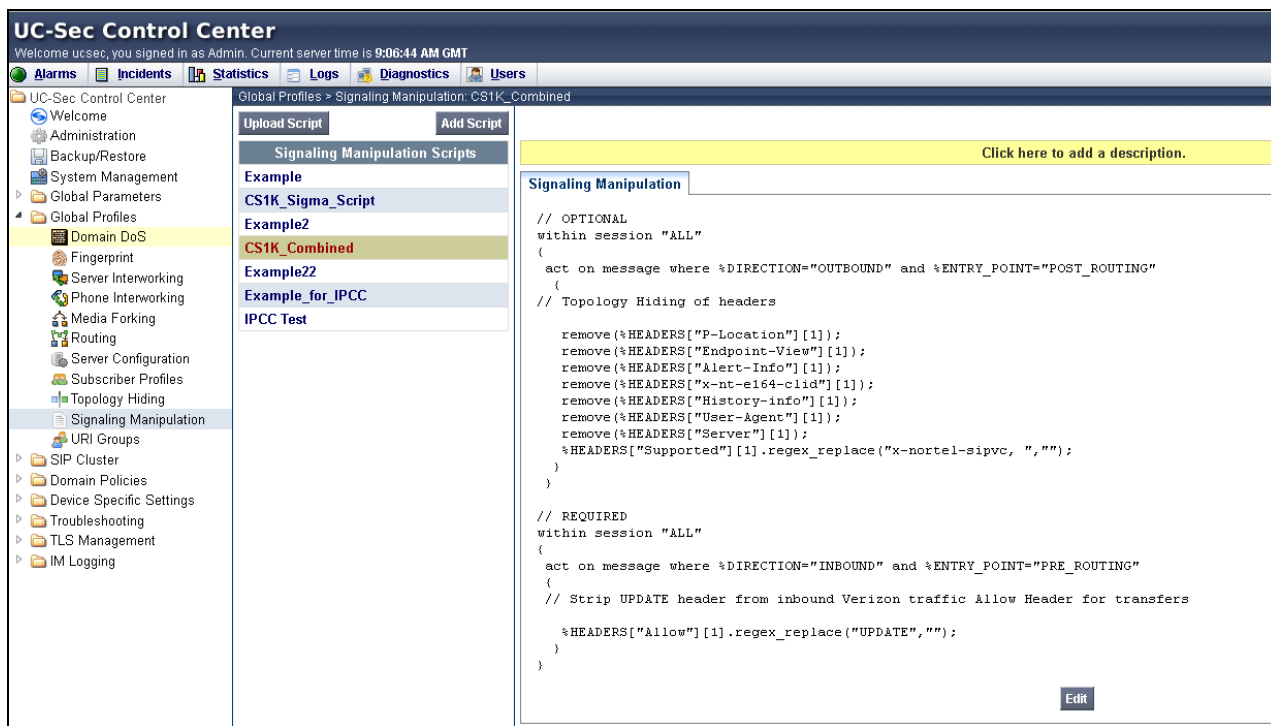
In the second part of this script beginning with the line **//REQUIRED**, these lines were included into the SigMa Script as a work-around to allow transfers off-net. Please see **Section 2.2** for more information and **Appendix 1** for the full text of this SigMa script.

```

1 // OPTIONAL
2 within session "ALL"
3 {
4   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
5   {
6     // Topology Hiding of headers
7
8     remove(%HEADERS["P-Location"][1]);
9     remove(%HEADERS["Endpoint-View"][1]);
10    remove(%HEADERS["Alert-Info"][1]);
11    remove(%HEADERS["x-nt-e164-clid"][1]);
12    remove(%HEADERS["History-info"][1]);
13    remove(%HEADERS["User-Agent"][1]);
14    remove(%HEADERS["Server"][1]);
15    %HEADERS["Supported"][1].regex_replace("x-nortel-sipvc, ", "");
16  }
17 }
18
19 // REQUIRED
20 within session "ALL"
21 {
22   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
23   {
24     // Strip UPDATE header from inbound Verizon traffic Allow Header for transfers
25
26     %HEADERS["Allow"][1].regex_replace("UPDATE", "");
27   }
28 }
29

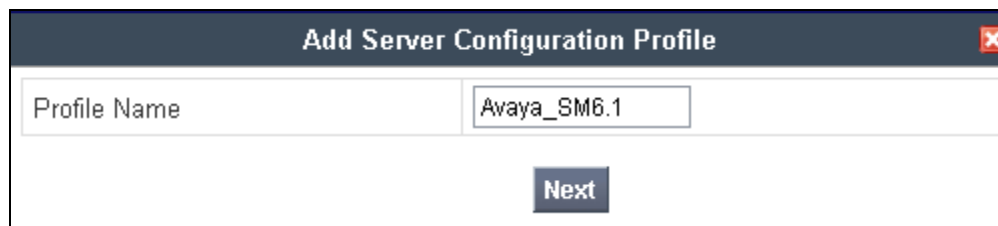
```

The following screen shows the finished Signaling Manipulation Script **CS1k_Combined**. This script will later be applied to the Verizon Server Configuration in **Section 7.3.6**. The details of these script elements can be found in **Appendix A**.



7.3.5 Server Configuration

Servers are defined for each server connected to the ASBCE. In this case, Verizon is connected as the Trunk Server and Session Manager is connected as the Call Server. To define the Session Manager server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter a profile name in the pop-up menu.



In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module.
- **Supported Transports:** Select **TCP** and **UDP**. This is the transport protocol used in the ASBCE Entity Link on Session Manager configured in **Section 6.5**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the ASBCE Entity Link on Session Manager configured in **Section 6.5**.

Click **Next** to continue.

Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.

The image shows two side-by-side screenshots of the 'Add Server Configuration Profile' wizard.

Left Window: Add Server Configuration Profile - General

- Server Type:** Call Server (selected in a dropdown)
- IP Addresses / Supported FQDNs:** 10.80.150.206 (text input)
- Supported Transports:** ☒ TCP, ☒ UDP, ☐ TLS
- TCP Port:** 5060
- UDP Port:** 5060 (highlighted with a red border)
- TLS Port:** (empty)

Buttons: Back, Next

Right Window: Add Server Configuration Profile - Authentication

- Enable Authentication:** ☐ (unchecked)
- User Name:** (empty text input)
- Realm:** (empty text input)
- Password:** (empty text input)
- Confirm Password:** (empty text input)

Buttons: Back, Next

In the new window that appears, **OPTIONS** were only configured for Session Manager. Enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds ASBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.3.3**. For **Signaling Manipulation Script** select a script if desired. Use default values for all remaining fields. Click **Finish** to save the configuration.

The image shows two side-by-side configuration windows. The left window, titled 'Edit Server Configuration Profile - Heartbeat', contains the following fields: 'Enable Heartbeat' (checked), 'Method' (dropdown set to 'OPTIONS'), 'Frequency' (text box with '60' and 'seconds' label), 'From URI' (text box with 'ping@10.80.140.141'), 'To URI' (text box with 'ping@10.80.150.206'), 'TCP Probe' (checkbox), and 'TCP Probe Frequency' (text box with 'seconds' label). The right window, titled 'Edit Server Configuration Profile - Advanced', contains: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown set to 'Avaya'), 'Signaling Manipulation Script' (dropdown set to 'None'), and 'TCP Connection Type' (radio buttons for 'SUBID', 'PORTID', and 'MAPPING', with 'SUBID' selected). Both windows have a 'Finish' button at the bottom right.

7.3.6 Server Configuration for Verizon IP Trunk

To define the Verizon IP Trunk, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and repeat the instructions above with appropriate settings.

The image shows a window titled 'Add Server Configuration Profile'. It has a single text input field labeled 'Profile Name' containing the text 'Vz_IPT'. Below the input field is a 'Next' button.

The screen below shows the General parameter settings for the “Vz_IPT” server configured as **Trunk Server**, with Verizon IP Address, transport, and port:

Global Profiles > Server Configuration: Vz_IPT

Profile

- Avaya_SM6.2
- Vz_IPT**
- Avaya_SM6.1
- default
- IPCC_Service

General | Authentication | Heartbeat | Advanced

General	
Server Type	Trunk Server
IP Addresses / FQDNs	172.30.209.21
Supported Transports	UDP
UDP Port	5071

Edit

The following screens show the settings in the **Authentication** and the **Heartbeat** tabs (note that external OPTIONS to Verizon are enabled in this configuration also):

Add Server Configuration Profile - Authentication

Enable Authentication ☐

User Name

Realm

Password

Confirm Password

Back **Next**

Edit Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method **OPTIONS**

Frequency seconds

From URI

To URI

TCP Probe ☐

TCP Probe Frequency seconds

Finish

In the **Advanced Tab**, select “Verizon_IPT” for **Interworking Profile** and “CS1K_Combined” as the **Signaling Manipulation Script** as shown below:

Global Profiles > Server Configuration: Vz_IPT

Profile

- Avaya_SM6.2
- Vz_IPT**
- Avaya_SM6.1
- default
- IPCC_Service

General | **Authentication** | **Heartbeat** | **Advanced**

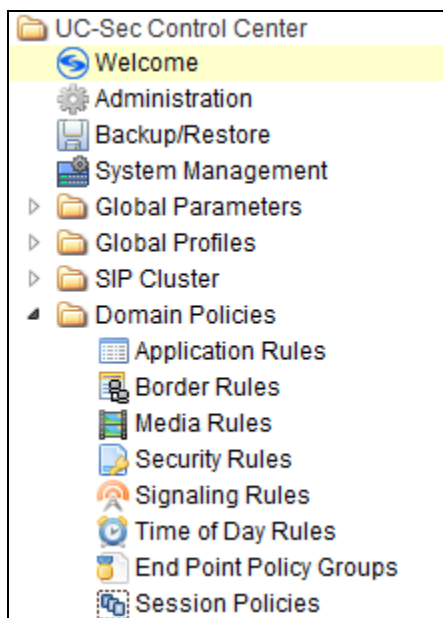
Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon_IPT
Signaling Manipulation Script	CS1K_Combined
UDP Connection Type	SUBID

Edit

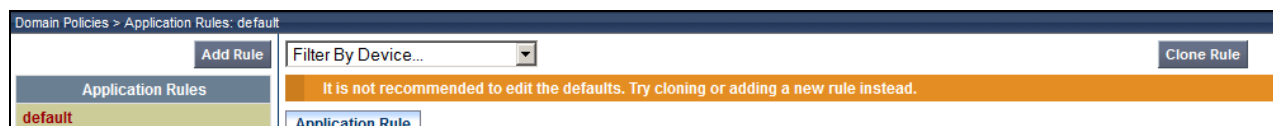
Click **Finish** to save changes (not shown).

7.4. Domain Policies – Application Rule

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below.



In the sample configuration, a single application rule was created by cloning the default rule called “default”. Select the default rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “Vz_App_Rule” as shown below. Click **Finish**.



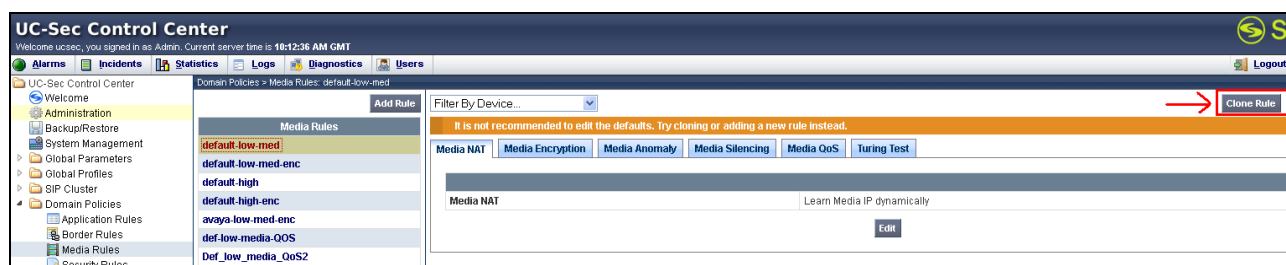
Select the newly created rule and click the **Edit** button (not shown). In the resulting screen, change the default **Maximum Concurrent Sessions** to 2000, the **Maximum Session per Endpoint** to 2000. Click **Finish**.

Application Rule				
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		
Miscellaneous				
CDR Support	None			
IM Logging	No			
RTCP Keep-Alive	No			

7.5. Domain Policies – Media Rules

Select **Domain Policies** → **Media Rules** from the left-side menu as shown below.

In the sample configuration, a single media rule was created by cloning the default rule called “**default-low-med**”. Select the default-low-med rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “**default-low-med-QoS**” as shown below. Click **Finish**.

Clone Rule	
Rule Name	default-low-med
Clone Name	default-low-med-QoS
<input type="button" value="Finish"/>	

Select the newly created rule, select the **Media QoS** tab, and click the **Edit** button (not shown). In the resulting screen, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

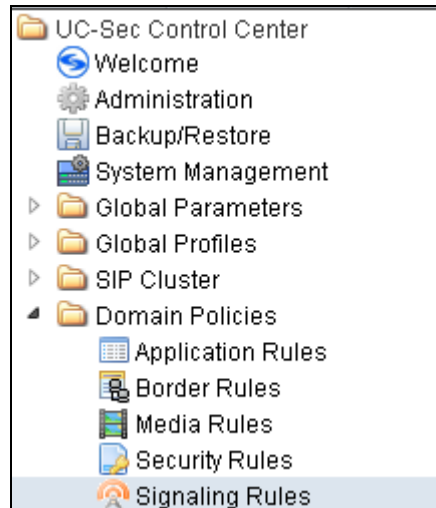
Media QoS			
Media QoS Reporting			
RTCP Enabled	<input type="checkbox"/>		
Media QoS Marking			
Enabled	<input checked="" type="checkbox"/>		
<input type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
<input checked="" type="radio"/> DSCP			
Audio	EF		101110
Video	EF		101110
Finish			

When configuration is complete, the “**default-low-med-QoS**” media rule **Media QoS** tab appears as follows.

Domain Policies > Media Rules: default-low-med-QoS	
<div> Add Rule Filter By Device... Rename Rule Clone Rule Delete Rule </div> <div> Click here to add a description. </div> <div> Media NAT Media Encryption Media Anomaly Media Silencing Media QoS Turing Test </div>	<div> Media QoS Reporting </div> <div> RTCP Enabled <input type="checkbox"/> </div> <div> Media QoS Marking </div> <div> Enabled <input checked="" type="checkbox"/> </div> <div> QoS Type DSCP </div> <div> Audio QoS </div> <div> Audio DSCP EF </div> <div> Video QoS </div> <div> Video DSCP EF </div>

7.6. Domain Policies – Signaling Rules

Select **Domain Policies** → **Signaling Rules** from the left-side menu as shown below.



Click the **Add Rule** button to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as “**Block_Hdr_Remark**”.

Signaling Rule	
Rule Name	Block_Hdr_Remark
Next	

In the subsequent screen (not shown), click **Next** to accept defaults. In the **Signaling QoS** screen, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down menu. In the sample configuration, “**AF32**” was selected for “Assured Forwarding 32.” Click **Finish** (not shown).

Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Value	AF32	011100

After this configuration, the new “Block_Hdr_Remark” will appear as follows.

Domain Policies > Signaling Rules: Block_Hdr_Remark		
Add Rule Filter By Device... Rename Rule Clone Rule Delete Rule		
Click here to add a description.		
General Requests Responses Request Headers Response Headers Signaling QoS		
Signaling QoS		<input checked="" type="checkbox"/>
QoS Type	DSCP	
DSCP	AF32	

7.7. Domain Policies – End Point Policy Groups

Select **Domain Policies** → **End Point Policy Groups** from the left-side menu as shown below.

Select the **Add Group** button.

Domain Policies > End Point Policy Groups: default-low	
Add Group Filter By Device...	
Policy Groups	It is not recommended to edit the defaults. Try adding a new group instead.

Enter a name in the **Group Name** field, such as “**default-low-remark**” as shown below. Click **Next**.

Policy Group	
Group Name	default-low-remark
Next	

In the sample configuration, defaults were selected for all fields, with the exception of **Application Rule** which was set to “**Vz_App_Rule**”, **Media Rule** which was set to “**default-low-med-QoS**”, and **Signaling Rule**, which was set to “**Block_Hdr_Remark**” as shown below. The selected application rule, non-default media rule and signaling rule were created in previous sections. Click **Finish**.

Edit Policy Set

Application Rule

Vz_App_Rule

Border Rule

default

Media Rule

def-low-media-QOS

Security Rule

default-low

Signaling Rule

Block_Hdr_Remark

Time of Day Rule

default

Finish

Once configuration is completed, the “default-low-remark” policy group will appear as follows.

Domain Policies > End Point Policy Groups: def_low_remark

Add Group

Filter By Device...

Rename Group
Delete Group

Policy Groups

default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
OCS-default-high
avaya-def-low-enc
def_low_remark

Click here to add a description.

Hover over a row to see its description.

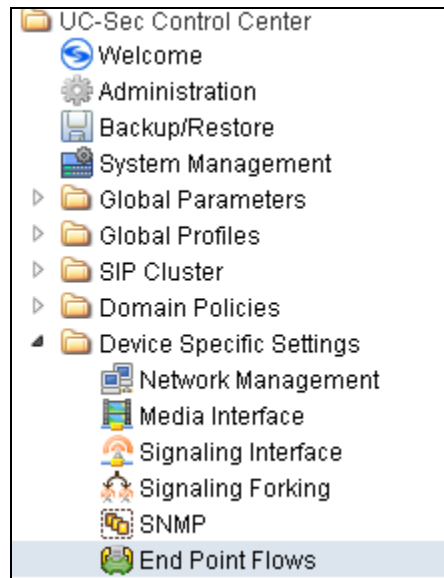
Policy Group

View Summary
Add Policy Set

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	Vz_App_Rule	default	def-low-media-QOS	default-low	Block_Hdr_Remark	default		

7.8. Device Specific Settings – End Point Flows

Select **Device Specific Setting** → **End Point Flows** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “**Vz_1**” in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.



The following screen shows the flow named “**Avaya_SM6.1**” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: Avaya_SM6.1

Criteria	
Flow Name	Avaya_SM6.1
Server Configuration	Avaya_SM6.1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Slg_Outside_to_Vz
Signaling Interface	Sig_Inside_to_CPE
Media Interface	Int_Media_to_CPE
End Point Policy Group	def_low_remark
Routing Profile	Vz_IPT
Topology Hiding Profile	Avaya
File Transfer Profile	None
Finish	

Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named “Verizon_IP_Trunk” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: Verizon_IP_Trunk
✕

Criteria	
Flow Name	<div style="border: 1px solid red; padding: 2px;">Verizon_IP_Trunk</div>
Server Configuration	<div style="border: 1px solid #ccc; padding: 2px;">Vz_IPT ▾</div>
URI Group	<div style="border: 1px solid #ccc; padding: 2px;">* ▾</div>
Transport	<div style="border: 1px solid #ccc; padding: 2px;">* ▾</div>
Remote Subnet	<div style="border: 1px solid #ccc; padding: 2px;">*</div>
Received Interface	<div style="border: 1px solid #ccc; padding: 2px;">Sig_Inside_to_CPE ▾</div>
Signaling Interface	<div style="border: 1px solid #ccc; padding: 2px;">Sig_Outside_to_Vz ▾</div>
Media Interface	<div style="border: 1px solid #ccc; padding: 2px;">Ext_Media_to_Vz ▾</div>
End Point Policy Group	<div style="border: 1px solid #ccc; padding: 2px;">def_low_remark ▾</div>
Routing Profile	<div style="border: 1px solid #ccc; padding: 2px;">Route to SM6.1 ▾</div>
Topology Hiding Profile	<div style="border: 1px solid #ccc; padding: 2px;">Verizon_IPT ▾</div>
File Transfer Profile	<div style="border: 1px solid #ccc; padding: 2px;">None ▾</div>

Finish

The following screen summarizes the Server Flows configured in the sample configuration.

Device Specific Settings > End Point Flows: VZ_1

UC-Sec Devices

VZ_1

Subscriber Flows

Server Flows

Click here to add a row description.

Server Configuration: Avaya_SM6.1

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile
1	Avaya_SM6.1	*	*	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	Int_Media_to_CPE	def_low_remark	Vz_IPT	Avaya

Server Configuration: Vz_IPT

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile
1	Verizon_IP_Trunk	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	Ext_Media_to_Vz	def_low_remark	Route to SM6.1	Verizon_IPT

8. Verizon Business IP Trunk Service Offer Configuration

Information regarding Verizon Business IP Trunk service offer can be found at <http://www.verizonbusiness.com/us/products/voip/trunking/> or by contacting a Verizon Business sales representative.

The sample configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Test Lab. The Verizon Business IP trunk service was accessed via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

8.1. Fully Qualified Domain Name (FQDN)s

The following Fully Qualified Domain Names (FQDN)s were provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i>

8.2. DID Numbers Assigned by Verizon

Verizon provided DID numbers that could be called from the PSTN. These Verizon-provided DID numbers terminated to the Avaya CS1000E location via the Verizon IP Trunk Service. **Table 1** in Section 3 shows example Verizon DID numbers and the configurable association of the Verizon DID numbers with Avaya CS1000E users.

9. Verification Steps

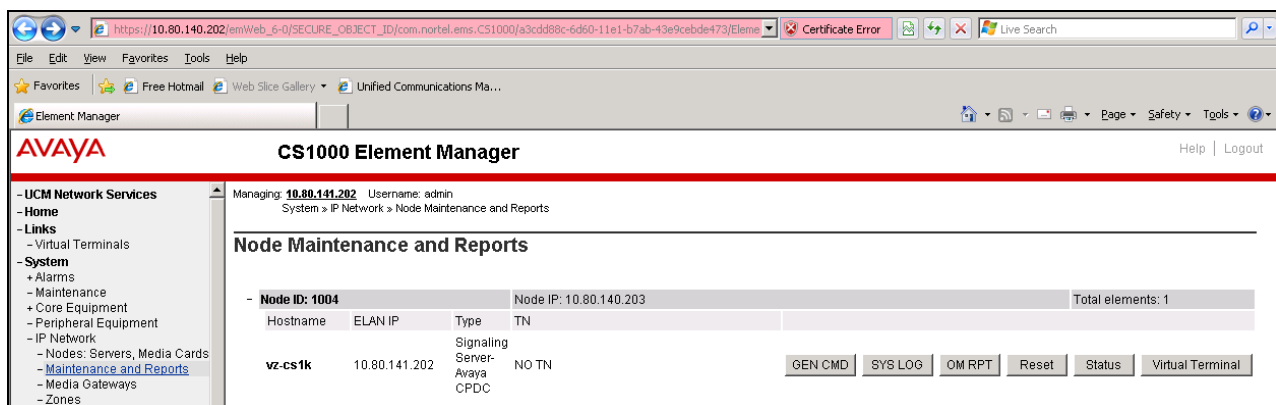
This section provides example verifications of the Avaya configuration with Verizon Business IP Trunk service.

9.1. Avaya Communication Server 1000E Verifications

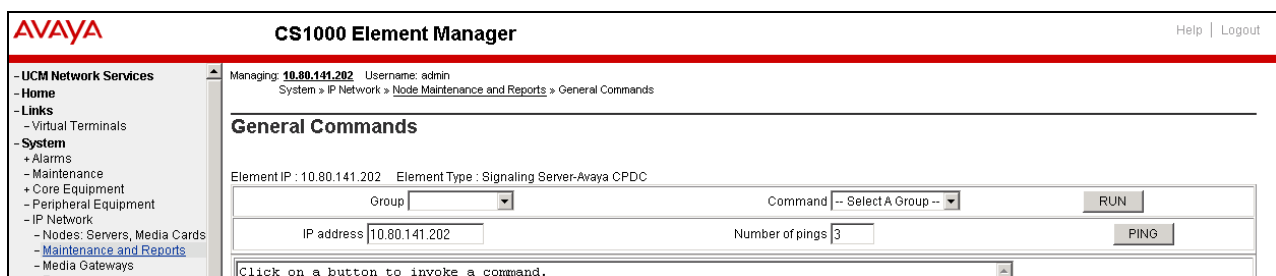
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

9.1.1 IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the **Gen CMD** button.



The **General Commands** page is displayed as shown below.



A variety of commands are available by selecting an appropriate **Group** and **Command** from the drop-down menus, and selecting **Run**.

To check the status of the SIP Gateway to Session Manager in the sample configuration, select “Sip” from the **Group** menu and “SIPGwShow” from the **Command** menu. Click **Run**. The example output below shows that the Session Manager (10.80.150.206, port 5060, TCP) has SIPNPM Status “Active”.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main panel is titled 'General Commands' and shows the command 'SIPGwShow' being executed on the 'Sip' group for the IP address '10.80.141.202'. The output displays the SIPNPM Status as 'Active' and provides details for the primary and secondary proxy servers, including IP addresses, ports, and transport protocols.

SIPNPM Status	
SIPNPM Status	: Active
Primary Proxy IP address	: 10.80.150.206
Primary Proxy port	: 5060
Primary Proxy Transport	: TCP
Secondary Proxy IP address	: 0.0.0.0
Secondary Proxy port	: 5060
Secondary Proxy Transport	: TCP
Primary Proxy2 IP address	: 10.80.150.206
Primary Proxy2 port	: 5060
Primary Proxy2 Transport	: TCP
Active Proxy	: Primary :Register Not Supported
Time To Next Registration	: 0 Seconds
Channels Busy / Idle / Total	: 0 / 32 / 32
Stack version	: 5.5.0.13
TLS Security Policy	: Security Disabled

As another example, the following screen shows the results of the “vtrkShow” Command from the “Vtrk” Group. The command was run with an active incoming call from the Verizon IP Trunk to an IP/Unistim telephone. Therefore, one channel is busy, and 63 idle.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar is the same as the previous screenshot. The main panel is titled 'General Commands' and shows the command 'vtrkShow' being executed on the 'Vtrk' group for the IP address '10.80.141.202'. The output displays a VTRK Summary with details about the trunk status, master status, registration node, protocol, and channel counts.

VTRK Summary	
VTRK status	: Active
Master status	: On
VTRK REG Node	: 1004
Protocol	: SIP SIPL
D-Channel	: 15
Customer	: 0
Channels Idle	: 63
Channels Busy	: 1
Channels Mbsy	: 0
Channels Pend	: 0
Channels Dsbl	: 0
Channels Ukwn	: 0

Below is the same call placed to a SIP extension. Notice that the Channels Busy is now 2 instead of 1.

AVAYA CS1000 Element Manager

Managing: **10.80.141.202** Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: **Vtrk** Command: **vtrkShow** Protocol: Start: Range: **RUN**

IP address: **10.80.141.202** Number of pings: **3** **PING**

```

-----
VTRK Summary
-----
VTRK status      : Active
Master status    : On
VTRK REG Node    : 1004
Protocol         : SIP SIPL
D-Channel        : 15
Customer         : 0
Channels Idle    : 62
Channels Busy    : 2
Channels Mbsy    : 0
Channels Pend    : 0
Channels Dsbl    : 0
Channels Ukwn    : 0
  
```

The next screen capture shows the output of the Command “SIPGWShowch” in Group “Sip” for channel 1, while an incoming call was active (using channel 1) from the Verizon IP Trunk Service to an IP-UNISTim phone. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “G_729A_20MS”. Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of ASBCE.

Managing: **10.80.141.202** Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: **Sip** Command: **SIPGwShowch** **Sip** **1** **RUN**

IP address: **10.80.141.202** Number of pings: **3** **PING**

```

Stack version          : 5.5.0.13
TLS Security Policy    : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used       : RPT
Channel tracing        : -1
Handle      Chan Type  Direction CallState SIPState      RxState TxState
-----
0xb7e0f418   1 VTRK      Terminate BUSY      Ringing Sent   Connected Connected
Codec
AirTime FS  MS Fax DestNum RemoteIP  URI Scheme
-----
G_729A_20MS      9 yes m  no  2000   10.80.140.141  ::              SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

The next screen capture shows an alternate way to view similar information, but in this case, by searching for calls involving a specific directory number. The screen shows the output of the **Command “SIPGWShownum”** in **Group “Sip”** where DN 2000 was specified. An incoming call was active from the Verizon IP Trunk Service to the IP-UNISTim phone with DN 2000. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “G_729A_20MS”. Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of the ASBCE.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main panel is titled 'General Commands' and shows the command 'SIPGWShownum' executed in the 'Sip' group for directory number '2000'. The output displays call details for a terminating call from 10.80.140.141 to 2000, using the G_729A_20MS codec.

```

Managing: 10.80.141.202 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Sip Command: SIPGWShownum SIP: 2000 RUN
IP address: 10.80.141.202 Number of pings: 3 PING

TLS Security Policy : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used : RPT
Channel tracing : -1
Calling/Called Party Number: 2000
Numbering Plan Indicator: Undefined
Type Of Number: Undefined

Handle Chan Type Direction CallState SIPState RxState TxState
-----
0xb7e0f418 1 VTRK Terminate BUSY Ringing Sent Connected Connected
Codec AirTime FS MS Fax DestNum RemoteIP URI Scheme
-----
G_729A_20MS 309 yes m no 2000 10.80.140.141 :: SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

The following screen shows the output of the **Command “SIPGWShowch”** in **Group “Sip”** for channel 1, when an outgoing call was active (using channel 1) from an IP UNISTim telephone to PSTN telephone number 13035387022 via the Verizon IP Trunk Service. Again, the use of G.729A to the inside IP Address (10.80.140.141) of the SBC can be observed.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar is the same as the previous screenshot. The main panel shows the command 'SIPGWShowch' executed in the 'Sip' group for channel '1'. The output displays channel status and call details for an outgoing call from 10.80.140.141 to 2000, using the G_729A_20MS codec.

```

Managing: 10.80.141.202 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Sip Command: SIPGWShowch SIP: 1 RUN
IP address: 10.80.141.202 Number of pings: 3 PING

Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 1 / 31 / 32
Stack version : 5.5.0.13
TLS Security Policy : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used : RPT
Channel tracing : -1

Handle Chan Type Direction CallState SIPState RxState TxState
-----
0xb7e0f418 1 VTRK Terminate BUSY Ringing Sent Connected Connected
Codec AirTime FS MS Fax DestNum RemoteIP URI Scheme
-----
G_729A_20MS 396 yes m no 2000 10.80.140.141 :: SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

Managing: **10.80.141.202** Username: admin
 System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Away CPDC

Group	<input type="text" value="SipLine"/>	Command	<input type="text" value="sigSetShowAll"/>	<input type="button" value="RUN"/>
IP address	<input type="text" value="10.80.141.202"/>	Number of pings	<input type="text" value="3"/>	<input type="button" value="PING"/>

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPV4 Endpoints -----							
2900	2900	252-00-09-00	1	0	0x9709da0		SIP Lines
Total User Registered = 1 V4 Registered = 1 V6 Registered = 0							

Managing: **10.80.141.202** Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group **lset** Command **lsetShow** Range **0** **500** **RUN**

IP address **10.80.141.202** Number of pings **3** **PING**

Set Information

IP Address	NAT	Model Name	Type	RegType	State	Up
10.80.140.135		1165E IP Deskphone	1165	Regular	busy	2

Total sets = 1

9.1.2 System Maintenance Commands

A variety of system maintenance commands are available by navigating to **System** → **Maintenance** using Element Manager. The user can navigate the maintenance commands using either the “Select by Overlay” approach or the “Select by Functionality” approach.

Managing: 10.80.141.202 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

The following screen shows an example where “Select by Overlay” has been chosen. The various overlays are listed, and the “LD 96 – D-Channel” is selected.

Managing: 10.80.141.202 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>
LD 30 - Network and Signaling
LD 32 - Network and Peripheral Equipment
LD 34 - Tone and Digit Switch
LD 36 - Trunk
LD 37 - Input/Output
LD 38 - Conference Circuit
LD 39 - Intergroup Switch and System Clock
LD 45 - Background Signaling and Switching
LD 46 - Multifrequency Sender
LD 48 - Link
LD 54 - Multifrequency Signaling
LD 60 - Digital Trunk Interface and Primary Rate Interface
LD 75 - Digital Trunk
LD 80 - Call Trace
LD 96 - D-Channel
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>
D-Channel Diagnostics
MSDL Diagnostics
TMDI Diagnostics

On the preceding screen, if **D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established “**EST**” and active “**ACTV**”.

Managing: **10.80.141.202** Username: admin
System » Maintenance » D-Channel Diagnostics

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button" value="Submit"/>
Test Interrupt Generation (TEST 100)		<input type="button" value="Submit"/>
Establish D-Channel (EST DCH)		<input type="button" value="Submit"/>

DCH DES
APPL_STATUS LINK_STATUS AUTO_RECV PDCH BDCH

015 VtrkNode1004 OPER EST ACTV AUTO

9.2. Wireshark Verifications

This section illustrates Wireshark traces for sample outbound and inbound calls using the sample configuration.

9.2.1 Example Outbound Call

This section illustrates an example outbound call from the Avaya CS1000E IP UNISTim user with Directory Number 2000 to PSTN telephone number 1-303-538-7024.

The following screen capture shows a Wireshark trace captured on the CPE private network, filtered on SIP messages sent from and to the IP Address of the Session Manager. The INVITE message is selected and the message header area is expanded to show the content of the SIP headers in the INVITE sent by the CS1000E and passed by Session Manager to the inside interface of the ASBCE. As can be observed, in the sample configuration, the CS1000E sends the DID number of the user placing the call in SIP headers such as the From and P-Asserted-Identity headers. The domain in the headers in source and destination headers is “avayalab.com” which the ASBCE will adapt to the source and destination domains expected by Verizon. Proprietary headers such as “x-nt-e164-clid” can be observed, and such headers will be removed by the ASBCE in the SigMa script that was added (See **Appendix 1**).

No.	Time	Source	Destination	Protocol	Info
17	5.143560	10.80.150.206	10.80.140.141	SIP/SDP	Request: INVITE sip:13035387024@avayalab.com;user=phone, w
20	5.144779	10.80.140.141	10.80.150.206	SIP	Status: 100 Trying
29	7.638486	10.80.140.141	10.80.150.206	SIP/SDP	Status: 183 Session Progress, with session description
36	7.649100	10.80.150.206	10.80.140.141	SIP	Request: OPTIONS sip:13035387024@10.80.140.141:5060;transp
52	7.725734	10.80.140.141	10.80.150.206	SIP	Status: 200 OK
267	9.150528	10.80.140.141	10.80.150.206	SIP/SDP	Status: 200 OK, with session description
277	9.160125	10.80.150.206	10.80.140.141	SIP	Request: ACK sip:13035387024@10.80.140.141:5060;transport=
448	10.303720	10.80.140.141	10.80.150.206	SIP	Request: BYE sip:7329450232@avayalab.com:5060;transport=tc
449	10.311352	10.80.150.206	10.80.140.141	SIP	Status: 200 OK

Frame 17: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits)	
Ethernet II , Src: Avaya_a3:a2:10 (90:fb:5b:a3:a2:10), Dst: IntelCor_cc:23:15 (00:1b:21:cc:23:15)	
Internet Protocol Version 4 , Src: 10.80.150.206 (10.80.150.206), Dst: 10.80.140.141 (10.80.140.141)	
Transmission Control Protocol , Src Port: 29818 (29818), Dst Port: sip (5060), Seq: 1461, Ack: 1, Len: 516	
[2 Reassembled TCP Segments (1976 bytes): #16(1460), #17(516)]	
Session Initiation Protocol	
Request-Line: INVITE sip:13035387024@avayalab.com;user=phone SIP/2.0	
Message Header	
Record-Route: <sip:7ee3cce8@10.80.150.206;transport=tcp;lr>	
Record-Route: <sip:10.80.150.205:15060;lr;sap=1041449358*1*016asm-callprocessing.sar-862564342-1347724374489-1876053234-1;tr>	
Record-Route: <sip:7ee3cce8@10.80.150.206;transport=tcp;lr>	
From: <sip:7329450232@avayalab.com;user=phone>;tag=4e44c90-cb8c500a-13c4-55013-1e053e-13f101b8-1e053e	
To: <sip:13035387024@avayalab.com;user=phone>	
Call-ID: 4e7c950-cb8c500a-13c4-55013-1e053e-45a4467a-1e053e	
CSeq: 1 INVITE	
Via: SIP/2.0/TCP 10.80.150.206;branch=z9hg4bk0A5096CD2EF0FFD401954147-AP;ft=293765	
Via: SIP/2.0/TCP 10.80.150.205:15070;branch=z9hg4bk0A5096CD2EF0FFD401954147	
Via: SIP/2.0/TCP 10.80.150.205:15070;branch=z9hg4bk0A5096CD2EF0FFD411954145	
Via: SIP/2.0/TCP 10.80.150.205:15070;branch=z9hg4bk0A5096CD2EF0FFD411954144	
Via: SIP/2.0/TCP 10.80.150.206;branch=z9hg4bk-1e053e-75447c12-19570aaa-AP;ft=215597	
Via: SIP/2.0/TCP 10.80.140.203:5060;branch=z9hg4bk-1e053e-75447c12-19570aaa	
Supported: 100rel, x-nortel-sipvc, replaces	
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-6.1.5.0.615006	
P-Asserted-Identity: <sip:7329450232@avayalab.com;user=phone>	
Privacy: none	
x-nt-e164-clid: +7329450232@avayalab.com;user=phone	
Alert-Info: <cid:external@avayalab.com>	
Contact: <sip:7329450232@avayalab.com:5060;maddr=10.80.140.203;transport=tcp;user=phone>	
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE	
Content-Length: 263	
Content-Type: application/sdp	
Route: <sip:10.80.140.141;transport=tcp;lr;phase=terminating>	
P-Location: SM;origlocname="Vz_CS1K";termlocname="ASBCE_1_Loc_140"	
Max-Forwards: 66	
Message Body	

The following screen shows the same Wireshark trace, but focuses on the message body. The body would typically contain MIME encapsulated application data for the SDP, “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” however, the Session Manager Adapter used in **Section 6.3.2** with the line **MIME=no** has removed it from the SDP before sending it to the ASBCE . The SDP has been expanded below so that it can be observed that the CS1000E SDP offer prefers G.729A and annexb=no.

Filter: sip && ip.addr==10.80.150.206					
No.	Time	Source	Destination	Protocol	Info
17	5.143560	10.80.150.206	10.80.140.141	SIP/SDP	Request: INVITE sip:13035387024@avayalab.com;user=phone, w
20	5.144779	10.80.140.141	10.80.150.206	SIP	Status: 100 Trying
29	7.638486	10.80.140.141	10.80.150.206	SIP/SDP	Status: 183 Session Progress, with session description
36	7.649100	10.80.150.206	10.80.140.141	SIP	Request: OPTIONS sip:13035387024@10.80.140.141:5060;transp
52	7.725734	10.80.140.141	10.80.150.206	SIP	Status: 200 OK
267	9.150528	10.80.140.141	10.80.150.206	SIP/SDP	Status: 200 OK, with session description
277	9.160125	10.80.150.206	10.80.140.141	SIP	Request: ACK sip:13035387024@10.80.140.141:5060;transport=
448	10.303720	10.80.140.141	10.80.150.206	SIP	Request: BYE sip:7329450232@avayalab.com:5060;transport=tc
449	10.311352	10.80.150.206	10.80.140.141	SIP	Status: 200 OK

[-] Frame 17: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits)
[-] Ethernet II, Src: Avaya_a3:a2:10 (90:fb:5b:a3:a2:10), Dst: IntelCor_cc:23:15 (00:1b:21:cc:23:15)
[-] Internet Protocol Version 4, Src: 10.80.150.206 (10.80.150.206), Dst: 10.80.140.141 (10.80.140.141)
[-] Transmission Control Protocol, Src Port: 29818 (29818), Dst Port: sip (5060), Seq: 1461, Ack: 1, Len: 516
[-] [2 Reassembled TCP Segments (1976 bytes): #16(1460), #17(516)]
[-] Session Initiation Protocol
[-] Request-Line: INVITE sip:13035387024@avayalab.com;user=phone SIP/2.0
[-] Message Header
[-] Message Body
[-] Session Description Protocol
[-] Session Description Protocol Version (v): 0
[-] Owner/Creator, Session Id (o): - 233 1 IN IP4 10.80.140.203
[-] Session Name (s): -
[-] Connection Information (c): IN IP4 10.80.140.135
[-] Time Description, active time (t): 0 0
[-] Media Description, name and address (m): audio 5200 RTP/AVP 18 0 8 101 111
[-] Connection Information (c): IN IP4 10.80.140.135
[-] Media Attribute (a): fmtp:18 annexb=no
[-] Media Attribute (a): rtpmap:101 telephone-event/8000
[-] Media Attribute (a): fmtp:101 0-15
[-] Media Attribute (a): rtpmap:111 X-nt-infreq/8000
[-] Media Attribute (a):ptime:20
[-] Media Attribute (a): sendrecv

The following screen shows a portion of the INVITE sent to Verizon from the outside of the ASBCE. The use of UDP and destination port 5071 can be observed. In the header portion of the message, observe that the Request-URI and To headers contain the Verizon domain “pcelban.avayalincroft.globalipcom.com” while the From and PAI headers contain the enterprise domain known to Verizon “adevc.avayalincroft.globalip.com.com”.

Filter: sip && ip.addr==2.2.2.2 Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
12	6.284165	2.2.2.2	172.30.209.21	SIP/SDP	Request: INVITE sip:13035387024@pcelban0001.avayalincroft.
15	6.364481	172.30.209.21	2.2.2.2	SIP	Status: 100 Trying
22	8.763358	172.30.209.21	2.2.2.2	SIP/SDP	Status: 183 Session Progress, with session description
28	8.776423	2.2.2.2	172.30.209.21	SIP	Request: OPTIONS sip:13035387024@172.30.209.21:5071;transp
36	8.851472	172.30.209.21	2.2.2.2	SIP	Status: 200 OK
303	10.253703	172.30.209.21	2.2.2.2	SIP/SDP	Status: 200 OK, with session description
309	10.266973	2.2.2.2	172.30.209.21	SIP	Request: ACK sip:13035387024@172.30.209.21:5071;transport=
846	12.952809	172.30.209.21	2.2.2.2	SIP	Request: BYE sip:7329450232@2.2.2.2:5060;transport=udp;use
850	12.962382	2.2.2.2	172.30.209.21	SIP	Status: 200 OK

<div>Frame 12: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)</div> <div>Ethernet II, Src: IntelCor_cc:23:11 (00:1b:21:cc:23:11), Dst: Cisco_5c:21:41 (00:04:9a:5c:21:41)</div> <div>Internet Protocol Version 4, Src: 2.2.2.2 (2.2.2.2), Dst: 172.30.209.21 (172.30.209.21)</div> <div>User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)</div> <div>Session Initiation Protocol <ul style="list-style-type: none"> Request-Line: INVITE sip:13035387024@pcelban0001.avayalincroft.globalipcom.com;user=phone SIP/2.0 Message Header <ul style="list-style-type: none"> From: <sip:7329450232@adevc.avaya.globalipcom.com;user=phone>;tag=4e404d0-cb8c500a-13c4-55013-1dfe3b-38ea04be-1dfe3b To: <sip:13035387024@pcelban0001.avayalincroft.globalipcom.com;user=phone> Cseq: 1 INVITE Call-ID: 4e7c0d0-cb8c500a-13c4-55013-1dfe3b-20402e18-1dfe3b Contact: <sip:7329450232@2.2.2.2:5060;transport=udp;user=phone> Record-Route: <sip:2.2.2.2:5060;ipcs-line=12042;lr;transport=udp> Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE Supported: 100rel, Replaces Max-Forwards: 66 Via: SIP/2.0/UDP 2.2.2.2:5060;branch=z9hg4bk-s1632-000658805596-1--s1632-Privacy: none P-Asserted-Identity: <sip:7329450232@adevc.avaya.globalipcom.com;user=phone> Content-Type: multipart/mixed;boundary=unique-boundary-1 Content-Length: 999 Message Body </div>

9.2.2 Example Inbound Call

This section illustrates an inbound call from PSTN telephone 303-538-1814 to Verizon IP Trunk DID 732-945-0232.

Filter: sip && ip.addr==2.2.2.2

No.	Time	Source	Destination	Protocol	Info
18	14.063912	172.30.209.21	2.2.2.2	SIP/SDP	Request: INVITE sip:7329450232@2.2.2.2:5060, with session
21	14.065897	2.2.2.2	172.30.209.21	SIP	Status: 100 Trying
24	14.134437	2.2.2.2	172.30.209.21	SIP	Status: 180 Ringing

Frame 18: 891 bytes on wire (7128 bits), 891 bytes captured (7128 bits)

- Ethernet II, Src: Cisco_5c:21:41 (00:04:9a:5c:21:41), Dst: IntelCor_cc:23:11 (00:1b:21:cc:23:11)
- Internet Protocol Version 4, Src: 172.30.209.21 (172.30.209.21), Dst: 2.2.2.2 (2.2.2.2)
- User Datagram Protocol, Src Port: powerschool (5071), Dst Port: sip (5060)
- Session Initiation Protocol
 - Request-Line: INVITE sip:7329450232@2.2.2.2:5060 SIP/2.0
 - Message Header
 - Via: SIP/2.0/UDP 172.30.209.21:5071;branch=z9hG4bkgf221f10b0105voc13o1.1
 - From: "AVAYA INC"<sip:3035387024@65.211.120.226;user=phone>;tag=192988269-1347725834800-
 - To: "Lincroft Lab LINCROFT LAB"<sip:7329450232@adevc.avaya.globalipcom.com>
 - Call-ID: Bw121714800150912-1493162661@65.211.120.226
 - CSeq: 626793753 INVITE
 - Contact: <sip:3035387024@172.30.209.21:5071;transport=udp>
 - Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
 - Accept: application/media_control+xml,application/sdp,multipart/mixed
 - Supported:
 - Max-Forwards: 69
 - Content-Type: application/sdp
 - Content-Length: 208
 - Message Body
 - Session Description Protocol
 - Session Description Protocol version (v): 0
 - Owner/Creator, Session Id (o): Broadworks 75640230 1 IN IP4 172.30.209.132
 - Session Name (s): -
 - Connection Information (c): IN IP4 172.30.209.132
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 10138 RTP/AVP 18 0 8 101
 - Media Attribute (a): rtpmap:101 telephone-event/8000
 - Media Attribute (a): fmtp:101 0-15
 - Media Attribute (a):ptime:20
 - Media Attribute (a): fmtp:18 annexb=no

The following screen shows the 200 OK in frame 37 expanded to show the contents of the SDP answer containing G.729A returned to Verizon. The use of the value 101 for any transmission of DTMF telephone events via RFC 2833 can also be observed.

Filter: sip && ip.addr==2.2.2.2 Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
32	17.877784	2.2.2.2	172.30.209.21	SIP	Request: OPTIONS sip:pcelban0001.avaya@incroft.globalipc
34	17.948121	172.30.209.21	2.2.2.2	SIP	Status: 200 OK
37	18.334490	2.2.2.2	172.30.209.21	SIP/SDP	Status: 200 OK, with session description

Frame 37: 1092 bytes on wire (8736 bits), 1092 bytes captured (8736 bits)					
Ethernet II, Src: IntelCor_cc:23:11 (00:1b:21:cc:23:11), Dst: Cisc0_5c:21:41 (00:04:9a:5c:21:41)					
Internet Protocol Version 4, Src: 2.2.2.2 (2.2.2.2), Dst: 172.30.209.21 (172.30.209.21)					
User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)					
Session Initiation Protocol					
Status-Line: SIP/2.0 200 OK					
Message Header					
Message Body					
Session Description Protocol					
Session Description Protocol version (v): 0					
Owner/Creator, Session id (o): - 236 1 IN IP4 2.2.2.2					
Session Name (s): -					
Connection Information (c): IN IP4 2.2.2.2					
Time Description, active time (t): 0 0					
Media Description, name and address (m): audio 35032 RTP/AVP 18 101 111					
Connection Information (c): IN IP4 2.2.2.2					
Media Attribute (a): fmtp:18 annexb=no					
Media Attribute (a): rtpmap:101 telephone-event/8000					
Media Attribute (a): fmtp:101 0-15					
Media Attribute (a): rtpmap:111 X-nt-inforeq/8000					
Media Attribute (a): pt=20					
Media Attribute (a): sendrecv					

The following screen capture shows a Wireshark trace filtered on SIP messages sent to and from the IP Address of Session Manager. The INVITE message from the ASBCE is selected and the message header is expanded for visibility. The message headers in the Request-URI, To and From now contain avayalab.com, the internal shared lab domain. Session Manager will adapt 732-945-0232 such that the call rings the IP UNISim telephone with Directory Number 2000, an IP UNISim telephone.

Filter: sip && ip.addr==10.80.150.206 Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
31	11.850719	10.80.140.141	10.80.150.206	SIP/SDP	Request: INVITE sip:7329450232@avayalab.com, with session
32	11.852928	10.80.150.206	10.80.140.141	SIP	Status: 100 Trying
34	11.918689	10.80.150.206	10.80.140.141	SIP	Status: 180 Ringing
51	16.118317	10.80.150.206	10.80.140.141	SIP/SDP	Status: 200 OK, with session description
63	16.346384	10.80.140.141	10.80.150.206	SIP	Request: ACK sip:2000@avayalab.com:5060;transport=tcp;user
776	20.935094	10.80.150.206	10.80.140.141	SIP	Request: OPTIONS sip:10.80.140.141;transport=tcp
792	21.008863	10.80.140.141	10.80.150.206	SIP	Status: 200 OK

Frame 31: 966 bytes on wire (7728 bits), 966 bytes captured (7728 bits)					
Ethernet II, Src: IntelCor_cc:23:15 (00:1b:21:cc:23:15), Dst: Avaya_a3:a2:10 (90:fb:5b:a3:a2:10)					
Internet Protocol Version 4, Src: 10.80.140.141 (10.80.140.141), Dst: 10.80.150.206 (10.80.150.206)					
Transmission Control Protocol, Src Port: entextnetwk (12001), Dst Port: sip (5060), Seq: 1, Ack: 2, Len: 912					
Session Initiation Protocol					
Request-Line: INVITE sip:7329450232@avayalab.com SIP/2.0					
Message Header					
From: "AVAYA INC" <sip:3035387024@avayalab.com;user=phone>;tag=192988269-1347725834800-					
To: "Lincroft Lab LINCROFT LAB" <sip:7329450232@avayalab.com>					
CSeq: 626793753 INVITE					
Call-ID: BwL21714800150912-1493162661@65.211.120.226					
Contact: <sip:3035387024@10.80.140.141:5060;transport=tcp>					
Record-Route: <sip:10.80.140.141:5060;ipcs-line=12274;r;transport=tcp>					
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY					
Supported:					
Max-Forwards: 69					
Via: SIP/2.0/TCP 10.80.140.141:5060;branch=z9hg4bk-s1632-000478797112-1--s1632-					
Accept: application/media_control+xml, application/sdp, multipart/mixed					
Content-Type: application/sdp					
Content-Length: 206					
Message Body					

9.3. System Manager and Session Manager Verification

This section contains verification steps that may be performed using System Manager for Session Manager.

9.3.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**.

From the list of monitored entities, select an entity of interest, such as “**Vz_ASBCE-1**”. Under normal operating conditions, the **Link Status** should be “**Up**” as shown in the example screen below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring								Help ?
SIP Entity, Entity Link Connection Status								
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.								
All Entity Links to SIP Entity: Vz_ASBCE-1								
Summary View								
1 Item Refresh								Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status	
► Show	ASM	10.80.140.141	5060	TCP	Up	200 OK	Up	

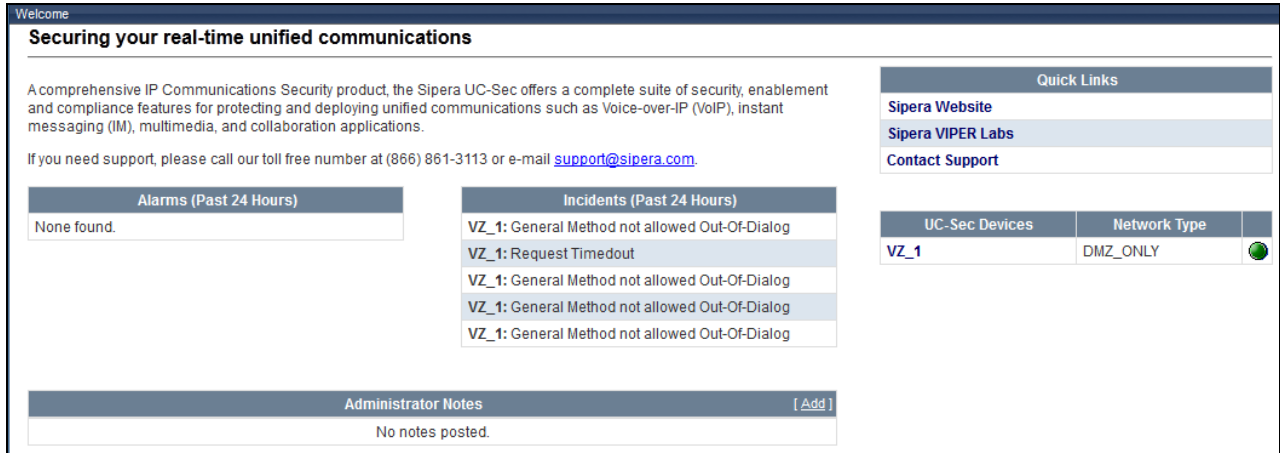
Return to the list of monitored entities, and select another entity of interest, such as “**Vz_CS1K_7.5**”. Under normal operating conditions, the **Link Status** should be “**Up**” as shown in the example screen below. In this case, “**Show**” under **Details** was selected to view additional information.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring								Help ?
hide navigation tree								
SIP Entity, Entity Link Connection Status								
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.								
All Entity Links to SIP Entity: Vz_CS1K_7.5								
Summary View								
1 Item Refresh								Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status	
▼ Hide	ASM	10.80.140.203	5060	TCP	Up	200 OK	Up	
Time Last Down		Time Last Up	Last Message Sent		Last Message Response		Last Response Latency (ms)	
Aug 23, 2012 3:19:06 PM MDT		Aug 23, 2012 3:21:23 PM MDT	Sep 13, 2012 11:06:01 AM MDT				9	

9.4. Avaya Session Border Controller for Enterprise Verification


9.4.1 Welcome Screen

The welcome screen shows alarms, incidents, and the status of all managed ASBCEs at a glance.



The screenshot shows the 'Welcome' page of the UC-Sec interface. The main heading is 'Securing your real-time unified communications'. Below this, a paragraph describes the product as a comprehensive IP Communications Security product. A support contact link is provided. The page is divided into three main sections: Alarms (Past 24 Hours), Incidents (Past 24 Hours), and a table of UC-Sec Devices. The Alarms section shows 'None found'. The Incidents section lists five incidents, all with the message 'VZ_1: General Method not allowed Out-Of-Dialog'. The UC-Sec Devices table shows one device, 'VZ_1', with a status of 'DMZ_ONLY' and a green indicator light. A 'Quick Links' section on the right contains links to the Spera Website, Spera VIPER Labs, and Contact Support. An 'Administrator Notes' section at the bottom shows 'No notes posted.'

Quick Links	
Spera Website	
Spera VIPER Labs	
Contact Support	

UC-Sec Devices	Network Type	
VZ_1	DMZ_ONLY	

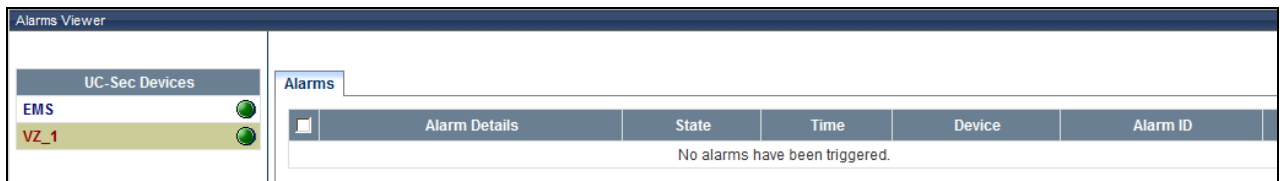
9.4.2 Alarms

A list of the most recent alarms can be found under the **Alarms** tab on the top left bar.



The screenshot shows the top bar of the UC-Sec Control Center. It features a dark blue header with the text 'UC-Sec Control Center' and 'Welcome ucsec, you signed in as Admin. Current server time is 3:45:21 PM GMT'. Below the header is a navigation bar with icons and labels for 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'.

Alarms Viewer:



The screenshot shows the 'Alarms Viewer' interface. On the left, there is a sidebar with a 'UC-Sec Devices' section containing 'EMS' and 'VZ_1', both with green indicator lights. The main area is titled 'Alarms' and contains a table with columns: 'Alarm Details', 'State', 'Time', 'Device', and 'Alarm ID'. The table is currently empty, with the message 'No alarms have been triggered.' displayed below the header.

Alarm Details	State	Time	Device	Alarm ID
No alarms have been triggered.				

9.4.3 Incidents

A list of all recent incidents can be found under the **Incidents** tab at the top left next to the **Alarms** tab.

Incidents Viewer:

Incident Viewer

Device

All

 Category

All

Clear Filters

Refresh

Show Chart

Generate Report

Displaying results 1 to 15 out of 712.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
BYE Message Out of Dialog	665258355113357	2/29/12	11:58 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665258344177160	2/29/12	11:58 AM	Policy	VZ_1	Request Timeout
BYE Message Out of Dialog	665258321513229	2/29/12	11:57 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
ACK Message Out of Dialog	665255354911409	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
REINVITE Message Out of Dialog	665255354909959	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665254922012124	2/29/12	10:04 AM	Policy	VZ_1	Request Timeout
Server Heartbeat	665000194930633	2/23/12	12:33 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	66500000924145	2/23/12	12:26 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664988030831612	2/23/12	5:47 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938207935094	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938196326749	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938193902637	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938182323645	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664916847577761	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664916833545584	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is failed

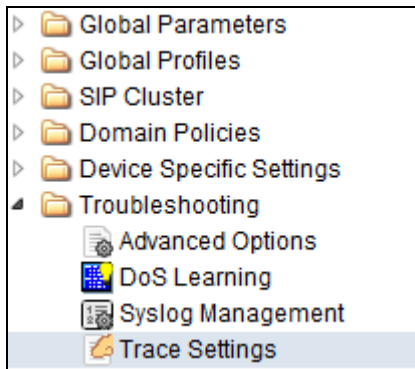
<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the **Incidents** viewer:

Incident Information			
General Information			
Incident Type	Server Heartbeat	Category	Policy
Timestamp	February 23, 2012 12:33:09 PM GMT	Device	VZ_1
Cause	Server Heartbeat is UP		
Message Data			
Response Code	200	Transport	TCP
Call ID	8d57142cb6a4bb2db3ab5301a040b218shiepaertab	From	sip:ping@avayalab.com
To	sip:ping@avayalab.com	Source IP	10.80.140.160
Destination IP	10.80.140.141		

9.4.4 Tracing

To take a call trace, Select **Troubleshooting** → **Tracing** from the left-side menu as shown below.



Select the **Packet Capture** tab and set the desired configuration for a call trace, then press **Start Capture**. Only one interface can be selected at once, so only an inside or only an outside trace is possible.

Packet Trace	Call Trace	Packet Capture	Captures
Packet Capture Configuration			
Currently capturing	No		
Interface	A1		
Local Address (ip:port)	All :		
Remote Address (*, *:port, ip, ip:port)	*		
Protocol	All		
Maximum Number of Packets to Capture	1000		
Capture Filename	Test_trace.pcap		
Existing captures with the same name will be overwritten			
<div>Start Capture</div> <div>Clear</div>			

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, press the **Stop Capture** button at the bottom (not shown).

Select the **Captures** tab at the top and the capture will be listed. The user can select an listed entry under **File Name** and choose to open it with an application like Wireshark.

Packet Trace	Call Trace	Packet Capture	Captures	
				Refresh
File Name		File Size (bytes)	Last Modified	
Test trace_20120229160214.pcap		49,152	February 29, 2012 4:02:26 PM GMT	X

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 can be configured to interoperate successfully with Verizon Business IP Trunk service. This solution allows Avaya Communication Server 1000E users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

11. Additional References

This section references documentation relevant to these Applications.

11.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

- [1] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Issue 4, Feb 2011 available at <http://support.avaya.com/css/P8/documents/100082630>
- [2] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Issue 2.2, April 2011 available at <https://downloads.avaya.com/css/P8/documents/100120934>
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Issue 4.2, November 2011 available at <https://downloads.avaya.com/css/P8/documents/100120937>
- [4] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, November 2010 available at <https://downloads.avaya.com/css/P8/documents/100120857>

Avaya Communication Server 1000E

- [1] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, Issue 05.09
- [2] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, Issue 05.17
- [3] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.10
- [4] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, Issue 03.05
- [5] Signaling Server and IP Line Applications Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, Issue 03.12

Appendix 1: Sigma Script

```
// OPTIONAL
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    // Topology Hiding of P-Location header for subsequent re-INVITES

    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["Endpoint-View"][1]);
    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["x-nt-e164-clid"][1]);
    remove(%HEADERS["History-info"][1]);
    remove(%HEADERS["User-Agent"][1]);
    remove(%HEADERS["Server"][1]);
    %HEADERS["Supported"][1].regex_replace("x-nortel-sipvc, ", "");
  }
}

// REQUIRED
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    // Strip UPDATE header from inbound Verizon traffic Allow Header for transfers

    %HEADERS["Allow"][1].regex_replace("UPDATE", "");
  }
}
```

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.